Trabajo de Fin de Máster

Máster Universitario en Ingeniería Industrial

Análisis de viabilidad de una celda de memoria enmascarable basada en RRAMs para aplicaciones de seguridad

MEMORIA

Autor: Carlos Xabier Otaño del Prado
Director: Daniel Arumí Delgado
Co-director: Salvador Manich Bou

Convocatoria: Julio 2019

Escola Tècnica Superior
d'Enginyeria Industrial de Barcelona

Resumen

En el año 2008 se fabricó el primer elemento memristivo, constatando lo que en 1971 había postulado teóricamente el ingeniero eléctrico e informático Leon Chua. Desde entonces, se ha investigado exhaustivamente en laboratorios y centros de todo el mundo las posibles aplicaciones de estos nuevos dispositivos en la tecnología actual.

Un elemento memristivo o *memristor,* es un dispositivo electrónico pasivo que, junto con la resistencia, el condensador y la inductancia, forman los cuatro elementos básicos de los circuitos eléctricos. Se pueden implementar físicamente de diversas maneras, experimentando en este proyecto con una de ellas: las RRAMs (*Resistive Random Access Memory*). El principio de funcionamiento de estos dispositivos, desarrollado en el capítulo 4, consiste en la regeneración y ruptura parcial de un filamento conductor provocando que estos adquieran dos estados resistivos característicos: LRS, del inglés *"Low Resistive State"* y HRS, del inglés *"High Resistive State".*

El objetivo principal del proyecto es diseñar y simular una celda de memoria enmascarable de un bit para aplicaciones en seguridad hardware contra ataques invasivos como la ingeniería inversa. Para ello, se ha utilizado la configuración en serie de dos RRAMs que permiten enmascarar un bit mediante un método que se desarrollará en el presente trabajo.

Se confirman observaciones realizadas en diferentes publicaciones, y se toman como punto de partida para el análisis de la viabilidad de la celda de memoria enmascarable. En primer lugar, en el capítulo 5, se confirma con las RRAMs aisladas el efecto de la corriente de *"compliance"* de la operación de escritura de *set* sobre la ventana que tiene la RRAM entre sus dos estados resistivos (LRS y HRS). En segundo lugar, en el capítulo 6, se trabaja con las RRAMs configuradas en serie, confirmando experimentalmente que conmuta aquella que tiene una resistencia mayor cuando ambas se encuentran en estado resistivo bajo (LRS), y que lo hace durante todos los ciclos de la experimentación.

En los capítulos 7 y 8, se realiza una propuesta de circuito de control de la celda de memoria enmascarable y su simulación eléctrica, confirmando los resultados que se esperaban y, por lo tanto, concluyendo que es viable la realización de una celda de memoria enmascarable basada en dispositivos RRAMs en serie.

Para terminar, en el capítulo 9, se realiza un estudio económico con los costes, tanto de instrumentación como de recursos humanos, imputados al proyecto de investigación.

Abstract

In 2008 the first memristive element was manufactured, confirming what the electrical and computer engineer Leon Chua had theoretically postulated in 1971. Since then, the possible applications of these new devices in current technology have been exhaustively researched in laboratories and centers all over the world

A memristive element or memristor, is a passive electronic device which, together with resistor, capacitor and inductance, form the four basic elements of electrical circuits. They can be physically implemented in several ways, experimenting in this project with one of them: RRAM (*Resistive Random Access Memory*). The principle of operation of these devices, developed in chapter 4, consists in the regeneration and partial rupture of a conductive filament in order to acquire the two characteristic resistive states: LRS (Low Resistive State) and HRS (High Resistive State).

The main goal of the project is to design and simulate a one-bit masking memory cell for hardware security applications against invasive attacks such as reserve engineering. In order to do this, it has been used the serial configuration of two RRAMs, that allow masking a bit using a method that will be developed in this work.

Observations made in different publications are confirmed, and are taken as the starting point for the analysis of the viability of the masking memory cell. Firstly, in chapter 5, the isolated RRAM confirm the effect of the compliance current of the set writing operation on the window that the RRAM has between its two resistive states (LRS and HRS). Secondly, in chapter 6, two RRAMs are configured in series, experimentally confirming that switches the one with the highest resistance when both are in LRS, and that it does so during all the cycles of the experimentation.

In chapters 7 and 8, a proposal is made for a control circuit of the memory cell and its electrical simulation, confirming the expected results and therefore, concluding that it is feasible to make a masking memory cell based on RRAM devices.

To conclude, in chapter 9, an economic study is carried out with the costs attributed to the research project.

Sumario

Índice de figuras

Índice de tablas

Listado de acrónimos

BE: Bottom Electrode

CF: Conductive Filament

CMOS: Complementary Metal-Oxide-Semiconductor

EEPROM: Electrically Erasable Programmable Read Only Memory

FA: Fault-Injection Attack

GPIB: General Purpose Interface Bus

HRS: High Resistive State

Icomps: Corriente de *compliance* de la operación de *set*

Icomp(*forming*): Corriente de *compliance* de la operación de *forming*

IMB-CNM: Instituto de Microelectrónica de Barcelona – Centro Nacional de Microelectrónica

IoT: Internet of Things

LRS: Low Resistive State

PUF: Physical Unclonable Function

QinE: Quality in Electronics

RRAM: Resistive Random Access Memory

SCA: Side-Channel Attack

SMU: Source-Measurement Unit

SRAM: Static Random Access Memory

TE: Top Electrode

V_S: Tensión aplicada en la operación de *set*

V_{SET}: Tensión umbral en la que se produce la conmutación de HRS a LRS

V_R: Tensión aplicada en la operación de *reset*

V_{RESET}: Tensión umbral en la que se produce la conmutación de LRS a HRS

1. Prefacio

1.1. Motivación del proyecto

Este proyecto surge por la motivación del grupo de investigación *Quality in Electronics* (QinE) del departamento de Ingeniería Electrónica de la Universidad Politécnica de Cataluña (UPC), de utilizar elementos memristivos, de los que se profundizará en este trabajo, para desarrollar nuevas aplicaciones en el campo de la seguridad hardware. El grupo QinE, junto con el grupo de investigación *Advanced Thin Dielectric Films* (ATDF) del Instituto de Microelectrónica de Barcelona del Centro Nacional de Microelectrónica (IMB-CNM), realizaron publicaciones [1] [2] a partir de las cuáles se hizo una propuesta de trabajo para demostrar la viabilidad de una celda de memoria enmascarable de un bit basada en una tecnología de memorias no volátiles en desarrollo.

Además, mi motivación por la realización del presente Trabajo de Fin de Máster recae en el gran interés en el mundo de la investigación académica y el aprendizaje de nuevos conocimientos y aplicaciones en el ámbito de la electrónica, que es uno de los que más proyección de futuro tiene actualmente. Durante los cuatro años de Grado en Ingeniería en Tecnologías Industriales cursados en la Universidad Pública de Navarra, aprendí los conocimientos básicos de la electrónica, y en la UPC, cursando el Máster en Ingeniería Industrial, he podido complementar dichos conocimientos con otros más técnicos que me han permitido realizar este proyecto de manera adecuada y satisfactoria.

2. Introducción

Actualmente, 4388 millones de personas en el mundo tienen acceso a Internet, lo que supone casi un 60% [3] de la población mundial. Es un claro indicador de la alta conectividad que existe y del gran intercambio de información y datos, así como las grandes plataformas que permiten que esta conectividad sea una realidad. Y conectarse a Internet no sólo implica el uso del ordenador portátil o de sobremesa para navegar por la web, si no que estamos rodeados de aparatos electrónicos interconectados. Objetos personales de uso cotidiano como tarjetas de crédito/débito (en dónde se incluyen las nuevas funcionalidades ofrecidas por los teléfonos inteligentes que permiten el pago por móvil), *smartphones*, *smart-watches*, transacciones bancarias, información biométrica para el acceso a vehículos etc., u objetos utilizados en las industrias y en las empresas como los sensores, almacenan miles de millones de datos y son enviados y recibidos a través de la red sin que apenas nos demos cuenta. A esta interconexión, el gran volumen de datos y la amplia diversidad de dispositivos interconectados, lo llamamos Internet de las Cosas (del inglés, *"Internet of Things"*, IoT).

Muchos de estos dispositivos contienen información sensible (datos personales, datos bancarios, claves de seguridad o incluso datos médicos personales) que necesitan de una protección especial para la seguridad personal del usuario [4]. Por ello, a día de hoy se trabaja en modelos más sofisticados de encriptación de datos, tanto en seguridad software como en seguridad hardware. No obstante, a pesar de los avances que se han realizado en ambos tipos de seguridad y todas las medidas de protección que se han implantado en multitud de países, el informe realizado por la empresa J.P. Morgan [5] apunta que al menos un 78% de las empresas a nivel mundial fueron objeto de fraude de pago mediante tarjetas de crédito/débito en 2018. Por lo tanto, la seguridad es un tema de actualidad que está en continuo cambio y ha de renovarse tan rápido como lo hagan los *hackers* que intentan acceder a nuestra información.

Cada movimiento realizado en Internet, es registrado en forma de datos en inmensos bancos de información. Y pese a que cada vez las leyes son más estrictas en la protección personal de datos, estas son más difíciles de cumplir para las empresas, que los utilizan con fines lucrativos. Todos los datos que circulan por la red pueden ser comercializados, registrados o utilizados por alguna persona de manera malintencionada. Y no sólo aquellos que circulan por la red, sino también los que son almacenados en memorias de dispositivos electrónicos, los cuales pueden ser utilizados por atacantes si estos tienen acceso físico al dispositivo. Este tipo de ataques al hardware, cuya principal finalidad es la obtención de claves secretas, se pueden clasificar de dos formas [4]. En función de si es necesaria la manipulación o no del dispositivo, se clasifican en:

- Ataques pasivos: son aquellos que no necesitan de la manipulación del dispositivo para obtener información, sino que se utilizan las propiedades físicas del mismo para revelar datos valiosos. Ejemplos de este tipo de ataques son los que observan el tiempo de ejecución o el consumo de potencia.

- Ataques activos: son aquellos que manipulan el dispositivo para conseguir un funcionamiento anormal de forma que se pueda obtener información sensible a través de este comportamiento erróneo. Un ejemplo de este tipo de ataque es el cambio en la frecuencia de reloj del dispositivo a través de una señal externa.

Por otra parte, en función de si es posible que el atacante pueda acceder físicamente al interior del dispositivo y las conexiones de manera sencilla o no, se clasifican en [6]:

- Ataques invasivos: son aquellos que modifican el dispositivo para obtener información. Comienzan retirando el empaquetado para poder acceder directamente a sus pistas y componentes. Una vez conseguido este acceso, se pueden realizar los ataques, por ejemplo, situando una sonda en una pista del circuito. Un ataque invasivo muy utilizado es el de ingeniería inversa, que permite al atacante entender cómo funciona el dispositivo con el fin de aumentar las posibilidades de éxito en el robo de información.

- Ataques semi-invasivos: son aquellos que requieren de la retirada del encapsulado del dispositivo para acceder a su superficie, pero no es necesario el contacto eléctrico con sus pistas ni componentes para obtener información. Representan una gran amenaza actualmente ya que son casi tan efectivos como los ataques invasivos, pero su coste es menor, similar al de los ataques no invasivos. Los más utilizados actualmente son los que se basan en el uso de rayos ultravioleta, infrarrojos, escáner laser o imagen térmica.

- Ataques no invasivos: son aquellos que no modifican ni manipulan el dispositivo para obtener información y, como consecuencia, no precisan de un instrumental tan costoso como en el caso los ataques invasivos. Dentro de este tipo de ataques, se puede distinguir de dos tipos:

    - Los ataques activos no invasivos, llamados ataques por inserción de fallos (en inglés, *"Fault-injection Attacks"*, FA): consisten en la introducción de fallos en el dispositivo durante su operación con el objetivo de que revele la clave secreta.

    - Los ataques pasivos no invasivos, llamados ataques de canal lateral (en inglés, *"Side-Channel Attacks"*, SCA): son aquellos que observan el dispositivo en modo de funcionamiento normal (análisis del consumo de potencia, tiempos

de ejecución, radiación electromagnética…) con el objetivo de desvelar la clave secreta.

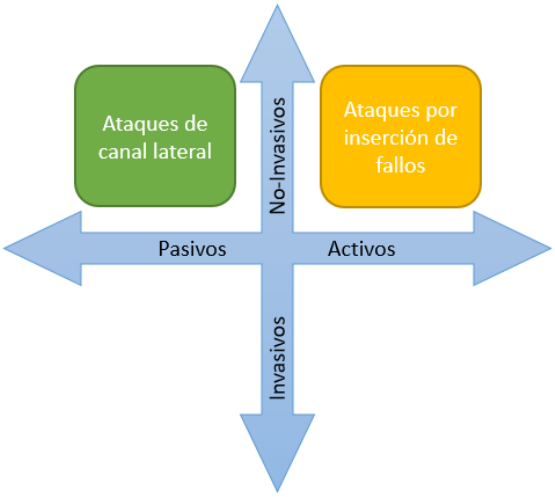


Figura 1. Clasificación de ataques contra el hardware. Fuente: [4]

Los ataques al hardware de un dispositivo han evolucionado con el paso de los años y cada vez son más potentes, representando una amenaza mayor contra la seguridad y privacidad de las personas. Además, no solo ha crecido el número de ataques que se realizan, si no que el número de atacantes también lo ha hecho.

Un componente actual clave para la seguridad en el hardware son las PUFs (del inglés, *"Physical Unclonable Functions"*) [7]. Su funcionamiento se basa en dos principios: en la aleatoriedad física que se produce al fabricar el dispositivo, y en la relación de una serie de pares "desafíos-respuesta" que no solo comprueba que la respuesta al software es correcta, sino que además se puede verificar a través de la PUF, que el hardware que intenta acceder al sistema es el legitimado para ello. Destacan por no requerir de una gran inversión de implementación debido a que el hardware utilizado es sencillo, y consumen menos energía y área de diseño que las EEPROM (del inglés, *"Electrically Erasable Programmable Read-Only Memory"*) o las SRAM (del inglés, *"Static Random Access Memory"*). Estas, se utilizan actualmente acompañadas de claves secretas y circuitos que evitan la intrusión de atacantes, sin embargo, son vulnerables a ataques como el FA. A pesar de que las PUFs son utilizadas en el mundo de la seguridad hardware, se muestran vulnerables ante cierto tipo de ataques como C. Helfmeier et al. desarrolla en [8].

Debido a las vulnerabilidades que muestran los sistemas utilizados para la protección de las memorias no volátiles, como los sistemas PUFs, se propone una nueva capa de seguridad hardware contra los ataques por ingeniería inversa, que aumentará el grado de seguridad de la información, ahorrará consumo de potencia y creemos que va a tener una gran proyección futura debido al uso de elementos memristivos emergentes en el mundo de la nanotecnología.

3. Planteamiento del problema

3.1. Modelo de ataque

En el capítulo 2 se han definido los diferentes tipos de ataque contra el hardware, aunque este trabajo se centrará en los ataques invasivos, en concreto aquellos que utilizan la ingeniería inversa contra chips de memorias no volátiles.

Por ello, se supondrá un modelo de atacante capaz de decapar el chip en donde se encuentre la celda de memoria, y observarla directamente mediante un microscopio electrónico. Además, podrá editar y manipular las conexiones del chip, así como realizar mediciones de la resistencia de las RRAMs (son los elementos memristivos utilizados para la elaboración de la celda de memoria que se explican en detalle en el capítulo 4) por separado y con el dispositivo sin alimentación.

Se excluyen a atacantes que sean capaces de medir la resistencia de las celdas de memoria cuando el chip está en estado activo, o de realizar medidas en las que se dé a conocer el valor de resistencia de más de una RRAM simultáneamente, debido a la complejidad de instrumentación requerida.

3.2. Objetivos del proyecto

El objetivo principal del trabajo es el análisis del comportamiento de dos RRAMs configuradas en serie y su aplicación para elaborar una celda de memoria enmascarable de un bit.

En primer lugar, se comprobará experimentalmente lo que postularon D. Arumí et al. [1] y que se utiliza como principio de realización de la celda de memoria enmascarable.

Una vez realizada esta comprobación experimental, se desarrolla el diseño propuesto y la simulación eléctrica de un circuito de control de la celda de memoria para comprobar su correcta funcionalidad.

4. Elementos memristivos

4.1. Introducción a los elementos memristivos

En 1971, el profesor Leon Chua [9] formuló teóricamente un nuevo elemento eléctrico al que denominó *"Memristor"*. Este lo definió como cualquier elemento eléctrico pasivo que, por sus características intrínsecas, relacionase la carga eléctrica (q) con el flujo magnético (Φ). Con este marco teórico proporcionado por el profesor L. Chua, expertos de todo el mundo investigaron y desarrollaron modelos de memristores capaces de convertir la teoría en práctica. Así, desde que en 2008 los laboratorios de Hewlett-Packard (HP) consiguieran fabricar el primer ejemplar de memristor [10], se ha puesto un gran interés en la investigación y desarrollo de prototipos e implementaciones de estos elementos.

Con la postulación teórica del memristor y su posterior confirmación experimental, se terminó por demostrar lo que los expertos en la materia llamaron "el cuarto elemento". Todos los elementos de los circuitos eléctricos de carácter pasivo pudieron ser relacionados entre sí mediante ecuaciones matemáticas y físicas. En la Figura 2 se muestra esta relación entre los cuatro elementos pasivos de los circuitos eléctricos:

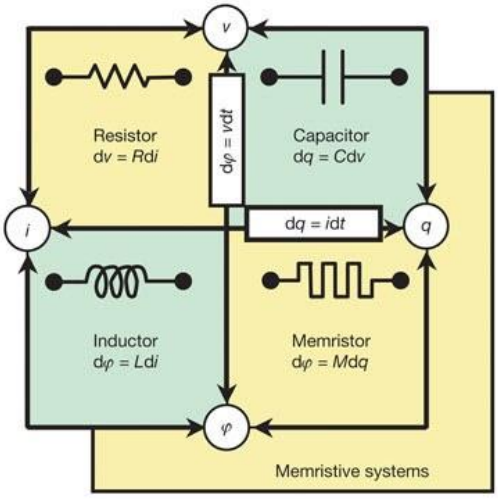


Figura 2. Relación entre los diferentes elementos pasivos de un circuito eléctrico. Fuente: [10]

4.2. Principio de funcionamiento de los elementos memristivos y física de las RRAMs

Como se ha explicado anteriormente, los memristores son elementos eléctricos de carácter pasivo con dos terminales o electrodos que relacionan la carga eléctrica (q) con el flujo magnético (Φ) (Ec.1). La variable que relaciona a ambas se denomina memristancia ($M(q)$), la cual depende de la carga eléctrica que circula o ha circulado por el dispositivo. Esta relación puede ser fácilmente transformada en otra ecuación (Ec. 2), que relaciona la intensidad ($i(t)$) con el voltaje ($v(t)$) a través de la misma variable. La memristancia, que tiene ohmios (Ω) como unidad de medida, representa la resistencia que varía de acuerdo con la carga eléctrica que circula o circuló entre los dos terminales del memristor.

$$M(q) = \frac{d\Phi}{dq} \qquad \text{(Ec. 1)}$$

$$v(t) = M\big(q(t)\big)\, i(t) \qquad \text{(Ec. 2)}$$

Las formas de implementación de elementos memristivos es variada y depende de diferentes factores, como la fabricación o su comportamiento interno. Pese a ello, todas tienen en común algo que les caracteriza como memristores: la conmutación resistiva. Esta consiste en el cambio entre dos o más estados resistivos que pueden adquirir los memristores en función de los estímulos externos que se apliquen [11]. Esta característica ha hecho emerger a un grupo de tecnologías para la realización de memorias no volátiles debido al poder que tienen de "recordar" el estado resistivo en el que se encuentran antes de ser desconectados de la fuente de alimentación. En este contexto, una de las tecnologías más prometedoras para la implementación de memristores es la basada en dispositivos RRAM (*"Resistive Random Access Memory"*). La mayoría de estos dispositivos se basan en un filamento conductor (en inglés, *"Conductive Filament"*, CF en adelante), capaz de romperse parcialmente y regenerarse en función de la polaridad del voltaje aplicado entre sus terminales. Esta ruptura parcial y regeneración del CF, hacen posible los dos estados resistivos de la tecnología RRAM utilizados en la elaboración de memorias no volátiles.

En este trabajo se ha experimentado con elementos memristivos basados en esta tecnología (a partir de aquí se referirá a estos dispositivos como RRAM). Estos han sido proporcionados por el grupo de investigación ATDF del IMB-CNM, y su estructura física

es del tipo MIM (*Metal-Insulator-Metal*) compuesta por TiN/Ti/HfO_2/W (Ver Figura 3). Tienen dos terminales o electrodos. El electrodo superior (en inglés, *"Top Electrode"*, TE en adelante) consiste en una capa de 200nm de grosor de TiN junto con una fina capa de Ti de 10nm de grosor, mientras que el electrodo inferior (en inglés, *"Bottom Electrode"*, BE en adelante) consiste en una capa con un grosor de 200nm de W.

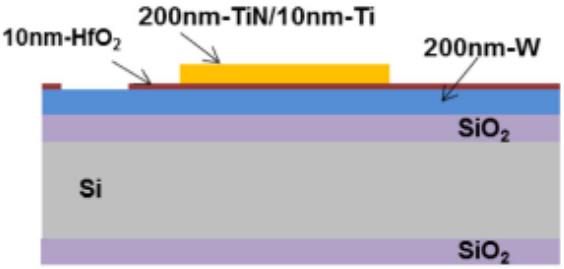


Figura 3. Sección esquemática de una RRAM

Las RRAMs utilizadas tienen un comportamiento bipolar, por lo que necesitan una tensión positiva para que se regenere el CF, y una tensión negativa para que el CF se rompa parcialmente. En la Figura 4 se muestra la oblea con la que se ha trabajado y en la Figura 5 las RRAMs utilizadas que hay en cada dado de la misma:

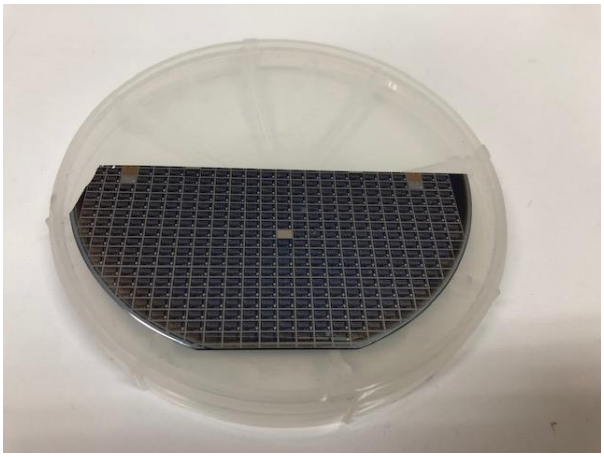


Figura 4. Oblea proporcionada por el IMB-CNM con la que se ha trabajado en el proyecto. Cada rectángulo que se aprecia en la oblea es un dado, y en ellos se encuentran las RRAMs

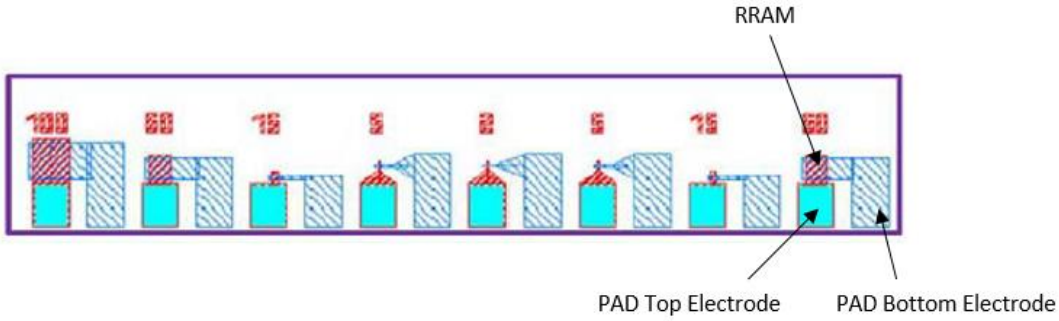


Figura 5. Las RRAMs son la intersección entre los dos PADs, y el número que hay sobre cada una de ellas es el área de intersección que forma la RRAM

4.3. Caracterización eléctrica de una RRAM

La palabra memristor proviene de la contracción de las palabras en inglés, *"memory"* y *"resistor"*. Por lo tanto, experimentalmente se comportan como resistencias capaces de recordar su estado resistivo cuando no tienen alimentación, como se ha explicado anteriormente. En la Figura 6 se muestra una curva I-V característica ideal de estos dispositivos mediante simulación:

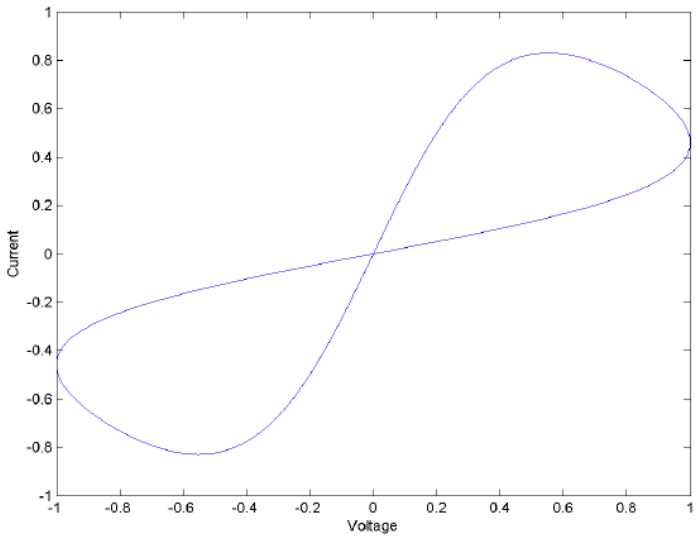


Figura 6. Curva I-V característica ideal de una RRAM. Fuente: [12]

Los dos estados resistivos no volátiles que caracterizan una RRAM son el estado resistivo alto (en inglés, *"High Resistive State"*, en adelante HRS) y el estado resistivo bajo (en inglés, *"Low Resistive State"*, en adelante LRS). El esquema básico de una RRAM se representa en la Figura 7:

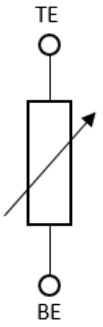


Figura 7. Esquema básico de una RRAM con sus electrodos (TE y BE)

El nivel de tensión que se aplique entre sus electrodos, así como su polaridad (positiva o negativa), tendrán un efecto en su estado resistivo. Por ello, se pueden diferenciar tres tipos de operaciones efectuadas sobre las RRAMs:

1. Operación de escritura de la RRAM: cuando la tensión entre TE y BE es positiva, se considera una operación de escritura de *"set"* y el estado resistivo con el que es configurada la RRAM es el LRS, mientras que, si la tensión aplicada entre estos terminales es negativa, la operación realizada es un *"reset"* y el estado resistivo final de la RRAM es el HRS. En la Figura 8, se representan estás operaciones. Los niveles de tensión máximos a los que deben ser sometidas, recomendados por el IMB-CNM, son 1,1V para la operación de *set*, y -1,4V para la operación de *reset*.

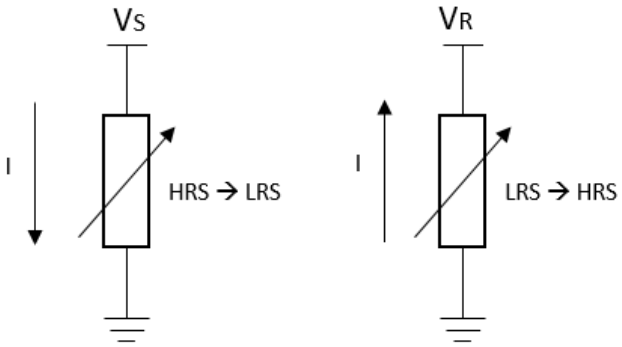


Figura 8. Operación de escritura de set y de reset

2. Lectura de la RRAM: se considera aquella operación que se realiza después de una operación de *set* o de *reset*, con el objetivo de conocer el estado resistivo (LRS o HRS) de la RRAM. El valor de tensión recomendado por el IMB-CNM para la lectura es de ±0,1V. Con este valor bajo de tensión, se asegura que no se afecta al estado resistivo, por lo que midiendo la corriente que circula entre los terminales y aplicando la Ley de Ohm, se puede obtener el valor de resistencia en los diferentes estados de la RRAM.

3. Operación de *"forming"*: La RRAM en su estado inicial no tiene formado el CF. Este filamento está constituido por vacantes de oxígeno que generan un camino de baja

resistencia entre sus electrodos. Al comienzo, todas las vacantes de oxígeno se encuentran en el elemento aislante (HfO_2) distribuidas de manera uniforme sobre este. Para generar el CF, es necesario aplicar una tensión positiva entre sus electrodos desde 0V hasta una tensión determinada, denominada tensión de *forming*. Esta operación es similar a la operación de *set*, pero aplicando un valor de tensión positiva mayor y únicamente se ha de realizar una vez en cada dispositivo al comienzo de la experimentación.

Teniendo en cuenta que la tecnología utilizada para fabricar las RRAMs está en fase de desarrollo e investigación, presentan una variabilidad en el valor de resistencia en sus estados resistivos a considerar. Esta variabilidad puede ser espacial cuando se produce entre diferentes dispositivos (en inglés, *"device-to-device"*), o temporal (en inglés, *"cycle-to-cycle"*) cuando se produce en un mismo dispositivo en diferentes operaciones de escritura (*set/reset*). Sobre la variabilidad se ha investigado y publicado diferentes artículos que explican este fenómeno [13] [14].

4.4. Aplicaciones de las RRAMs

Las RRAMs son consideradas como uno de los dispositivos emergentes con mayor proyección de futuro en aplicaciones tanto analógicas como digitales, sobretodo en chips de memoria, circuitos lógicos, redes neuronales y seguridad hardware. Entre sus características más importantes se encuentran, la velocidad de escritura/lectura, el bajo consumo de energía, la no-volatilidad, la escalabilidad y su compatibilidad con procesos de fabricación de tecnología CMOS.

4.4.1. Memorias

Actualmente, los chips de memorias no volátiles más conocidos son las *Flash*. Tienen una velocidad de escritura/lectura relativamente alta, pero con una limitada capacidad de integración en aplicaciones de memoria de gran densidad.

La utilidad de las RRAMs en el campo de las memorias no volátiles radica en el fenómeno de la conmutación resistiva. Como se ha visto anteriormente, son dispositivos que se pueden utilizar digitalmente ya que tienen dos estados resistivos (HRS o LRS). Aprovechando estas propiedades, se ha realizado una patente en EEUU [15], en la que se hace una propuesta de una memoria no volátil compuesta por RRAMs distribuidas en diferentes capas.

4.4.2. Circuitos lógicos

Las RRAMs permiten la construcción de puertas lógicas mediante su asociación en diferentes configuraciones (antiserie, antiparalelo, etc.), y su aparición ha hecho posible el desarrollo de

la lógica con puertas *IMPLY*, la cual es tan potente como la lógica con puertas NAND y NOR.

S. Kvatinsky et al. han realizado un sumador completo [16] y se describe un método para diseñar un *"crossbar"* con estos dispositivos. En otra publicación [17], se hace un mayor énfasis en la dificultad que tienen las RRAMs para afrontar la robustez necesaria en el desarrollo de una lógica de circuitos al completo debido al fenómeno de variabilidad. Es una aplicación todavía por desarrollar y en la que se sigue investigando.

4.4.3. Computación neuromórfica

Actualmente se está invirtiendo mucho en la investigación en computación neuromórfica debido al gran interés que existe en las empresas tecnológicas para desarrollar modelos de inteligencia artificial, el *machine learning*, la psicología cognitiva o la neurología. El carácter digital de las RRAMs cuando se opera con ellas con dos estados resistivos (LRS o HRS), cambia cuando estos dispositivos adoptan un mayor número de estados. En este caso, se dice que las RRAMs tienen un carácter analógico. Se utilizan para modelar experimentalmente el comportamiento en organismos, demostrando C.Li et al [18] que un circuito compuesto por estos elementos interconectados emulando una red neuronal, es capaz de aprender de un tren de pulsos y anticiparse a cuál será el siguiente estado.

4.4.4. Seguridad hardware

Debido a la característica I-V no lineal que poseen las RRAMs, es interesante el hecho de utilizarlas en el campo de la seguridad hardware. Aprovechando el fenómeno de variabilidad que poseen estos dispositivos cuando se experimenta con ellos, se ha prestado especial atención a esta aleatoriedad del comportamiento memristivo para utilizarlo en aplicaciones de seguridad [19].

Por ejemplo, en la generación aleatoria de bits [1] o en la fabricación de PUFs reconfigurables [20], las cuáles se basan en la variabilidad intrínseca de los mecanismos físicos de la RRAM para la protección del hardware, en vez de en la aleatoriedad producida en la propia fabricación.

5. Experimentación con RRAMs aisladas

5.1. Entorno de trabajo en el laboratorio

En el Laboratorio de Investigación De Electrónica nº2 (LIDE II) del grupo de investigación QinE, se dispone de los componentes necesarios para realizar todas las pruebas experimentales con las RRAMs proporcionadas por el IMB-CNM, tanto para la caracterización de los dispositivos aislados, como para la caracterización de los dispositivos en serie. En la Figura 9 se muestra un esquema de conexión de los diferentes componentes principales que forman el entorno de trabajo.

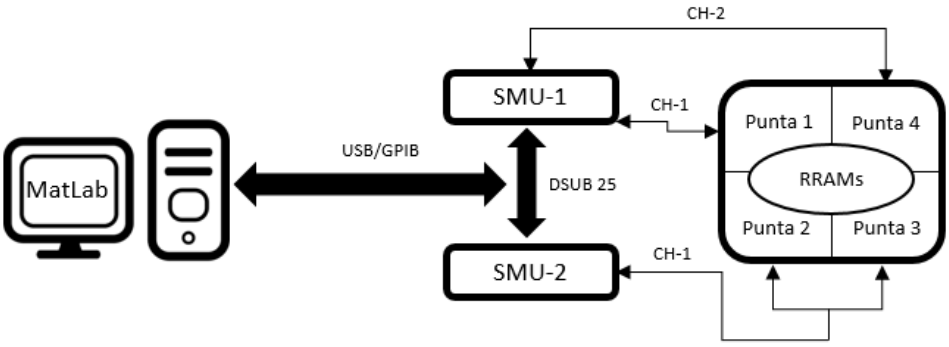


Figura 9. Conexión de los componentes principales utilizados para realizar los experimentos en el Laboratorio de Investigación De Electrónica nº2 (LIDE II)

5.1.1. Fuente de tensión y medida (SMU)

Para realizar las medidas y aplicación de los diferentes voltajes que se necesitan en cada una de las etapas de experimentación, se utilizan dos unidades de medición y fuente de tensión idénticas (en inglés, *"Source Measurement Unit"*, en adelante SMU). Ambas son de la marca *Keysight Technologies*, modelo B2912A, y se utilizan de forma que la SMU-1 hace la función de maestro y la SMU-2 hace la función de esclavo sincronizadas mediante el DSUB 25.

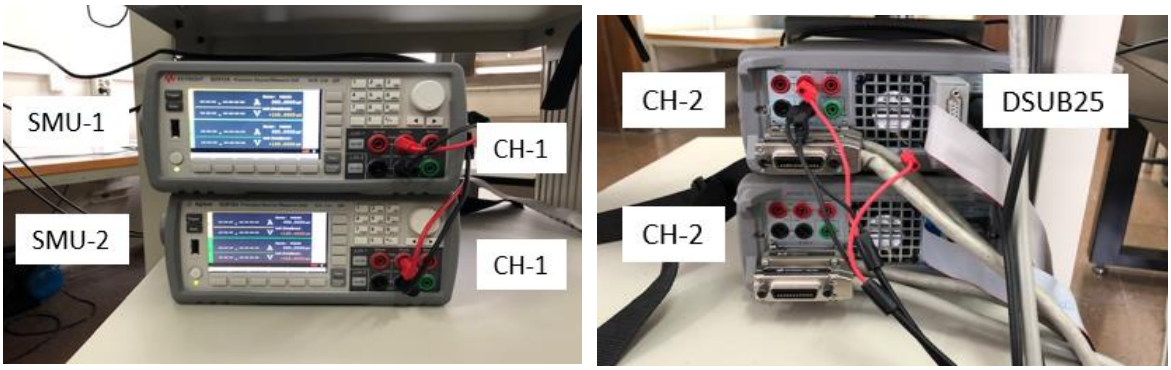


Figura 10. SMUs utilizadas para medir corriente y tensión, y aplicar voltaje durante los experimentos

Cada una de las SMUs tiene dos canales (CH-1 y CH-2), lo que hacen un total de cuatro canales. Sin embargo, se utilizan a efectos prácticos tres de ellos. En la Figura 9 se muestra la conexión de los canales de las SMUs con las puntas que se utilizan para la experimentación de las RRAMs.

5.1.2. Estación de puntas

La base de la estación de puntas es de la marca *Signatone*, y cuenta con los posicionadores DPP105-M/V-AI-S de la marca *Cascade/Microtech* y sus correspondientes puntas de prueba. Son necesarias para aplicar las tensiones que se han programado por software sobre las RRAMs. Tiene cuatro puntas, lo que permite realizar la configuración tanto en serie como en paralelo de dos RRAMs.

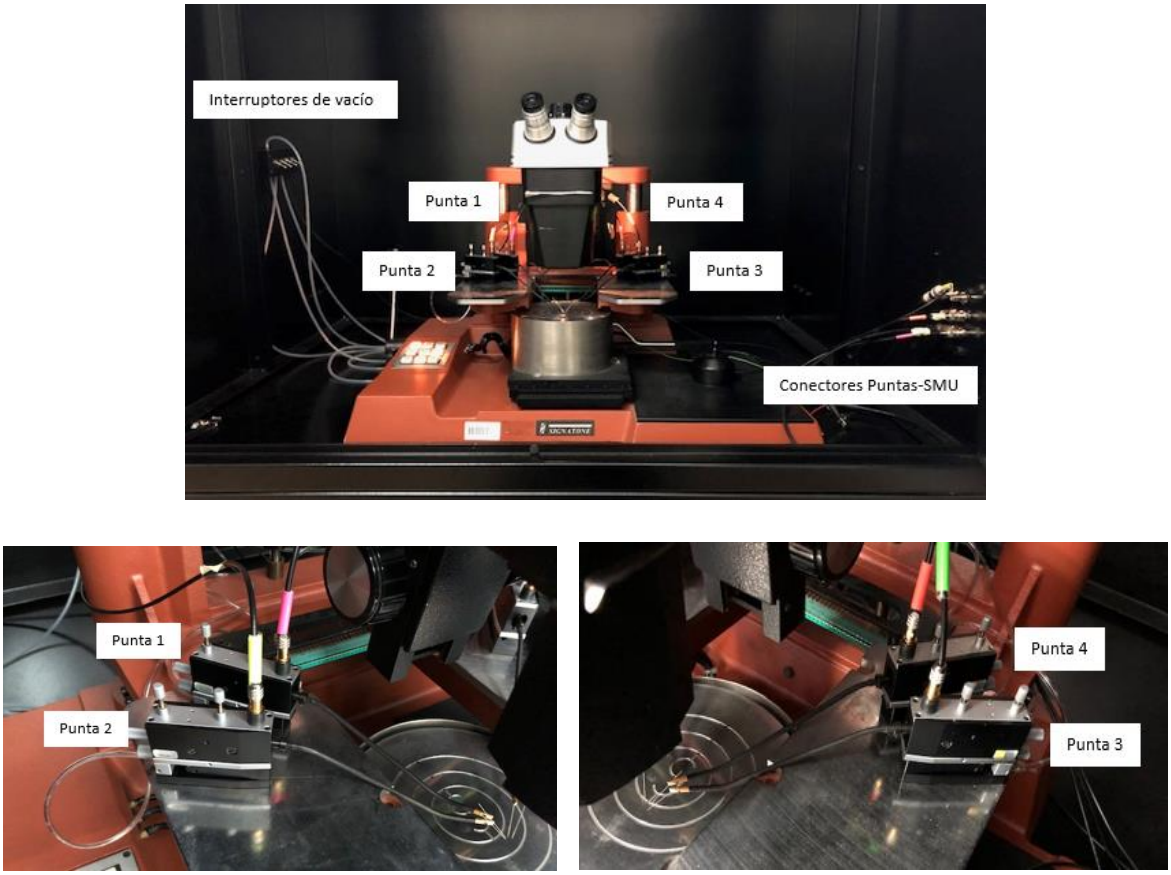


Figura 11. Estación de puntas, con los posicionadores y cada una de las puntas. Las puntas 1 y 2 se utilizan para una RRAM y las puntas 3 y 4 se utilizan para la otra RRAM

La estación está apoyada sobre una mesa neumática anti-vibraciones dentro de un armario metálico protector a modo de jaula de Faraday. La mesa neumática está accionada por un compresor y los posicionadores de las puntas están sujetos a la estación gracias a una bomba de vacío. El envoltorio metálico impide que el ruido electromagnético afecte a los dispositivos con los que se está experimentando en su interior.

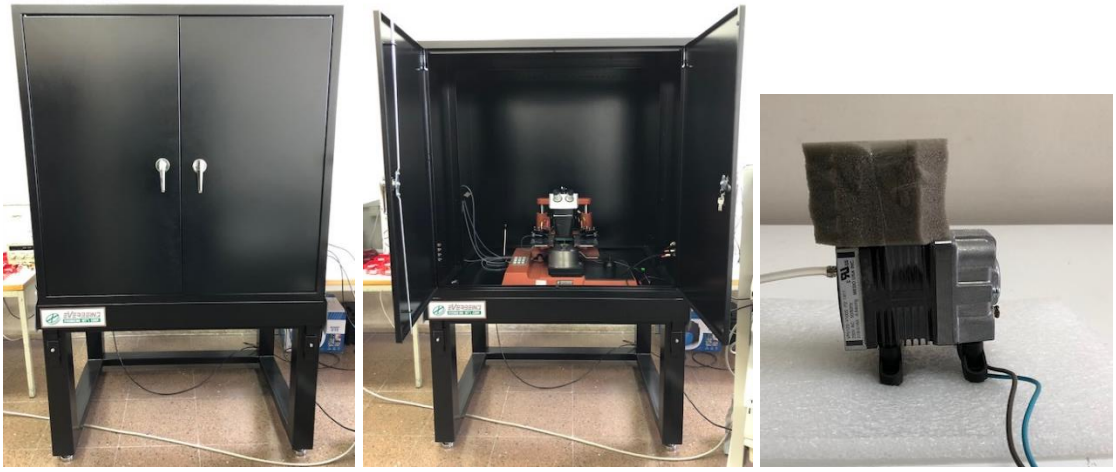


Figura 12. Envoltorio metálico y bomba de vacío

5.1.3. Ordenador con el software de programación

Para la realización de las diferentes pruebas experimentales sobre los dispositivos, se necesita un ordenador con el software *MatLab* en su versión R2018b. Con dicho software se han realizado todos los programas que permiten realizar las formas de onda, las medidas y el procesamiento de los datos adquiridos por las SMUs. Además del *MatLab*, es necesario tener instalado el controlador de las SMUs, el *Keysight Connection Expert 2019*. Este incluye las librerías que permiten programarlas, así como sus respectivas identificaciones y características propias.

Los programas fueron facilitados por el grupo de investigación QinE, y se han añadido fragmentos de código con el fin de optimizar las pruebas, diseñar nuevos experimentos y procesar los datos obtenidos. Se adjuntan en el Anexo A.

5.1.4. Comunicación USB/GPIB

La comunicación entre el ordenador en donde se ejecutan los programas y las SMUs, se realiza a través de un estándar bus de datos digital llamado GPIB (del inglés, *"General Purpose Instrumentation Bus"*).

Figura 13. Comunicación USB/GPIB

Gracias a este elemento, las SMUs y el ordenador están conectados y se puede enviar señales a las RRAMs, conectadas a las SMUs por medio de las puntas, como se aprecia en la Figura 9. Además, mediante el GPIB se pueden recibir en el ordenador los datos recogidos por las SMUs durante la experimentación.

5.2. Preparación de las RRAMs

Durante este trabajo, se han realizado pruebas en aproximadamente 400 RRAMs de la oblea. Requieren de una preparación previa a ser colocadas en serie, dividida en las diferentes etapas que se explican a continuación:

5.2.1. Etapa nº1: *Forming*

Se trata de una de las etapas más importantes, ya que la RRAM en su estado inicial no tiene formado el CF. Como se ha explicado anteriormente, para generar el CF, es necesario aplicar una tensión positiva entre TE y BE desde 0V hasta la tensión de *forming* ($V_{forming}$). Esta etapa está programada por software de manera que, en cada incremento de tensión, se mide la corriente que circula entre el TE y el BE del dispositivo con la SMU. Se vigila que dicha corriente no supere la corriente máxima recomendada por el IMB-CNM en esta etapa de preparación que es de 1mA, y se denomina corriente de *compliance* en el *forming* (Icomp(*forming*)). Cuando se alcanza este límite, el programa para automáticamente el aumento de tensión y se considera que el CF está formado. Los valores observados experimentalmente de $V_{forming}$, donde se genera el filamento, se encuentran en un rango típico entre 2,2V y 3V.

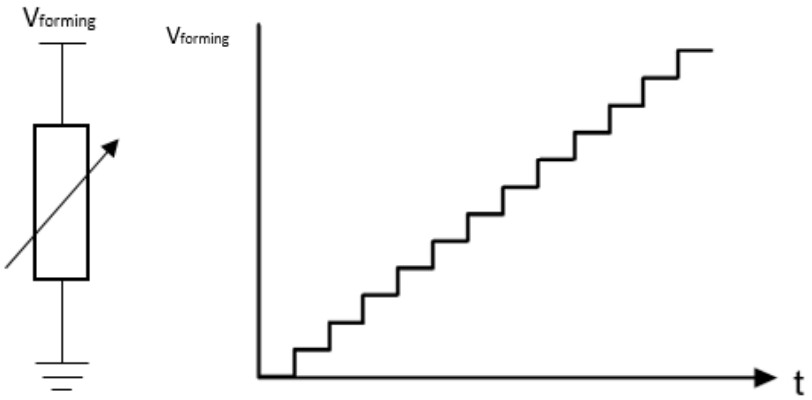


Figura 14. Forma de onda de la $V_{forming}$ aplicada entre los terminales de una RRAM

En la Figura 15 se aprecia experimentalmente como la intensidad que circula por el dispositivo al comienzo, cuando la tensión es baja, es del orden de decenas de nA, hasta que alcanza la $V_{forming}$ suficiente para formar el CF. Entonces, la intensidad que circula en el dispositivo es del orden de mA. Cuando este proceso se ha acabado, el CF se ha generado y el dispositivo queda configurado con el estado LRS. Por lo tanto, se obtiene un dispositivo capaz de ser configurado con dos estados resistivos en función de la operación de escritura (*set* o *reset*) que se realice: el estado de baja resistencia o LRS, en el que el CF está generado formando un camino de baja resistencia entre sus terminales, y el estado de alta resistencia o HRS, en donde el CF está roto parcialmente, creando un camino de alta resistencia entre TE y BE.

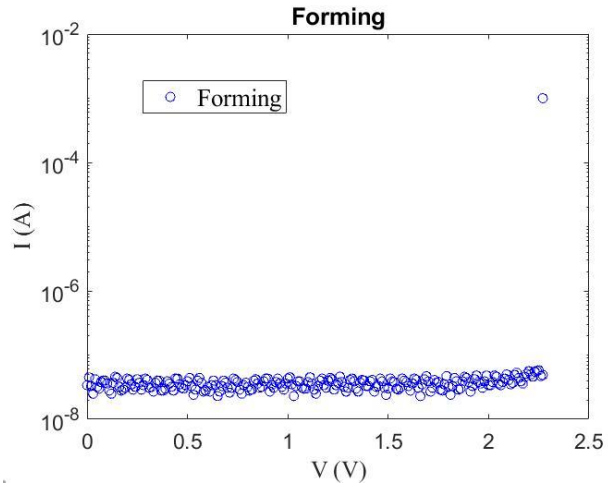


Figura 15. Resultado de la experimentación de la etapa de forming de una RRAM

5.2.2. Etapa nº2: Ciclos en continua

Una vez acabada la operación de *forming*, se continúa con la etapa nº2 que consiste en realizar ciclos en continua a un dispositivo. Se trata de aplicar tensión entre los electrodos de la RRAM en forma de doble rampa (de subida y de bajada) tanto para la operación de *set* como para la operación de *reset* durante varios ciclos de forma continua. En la Figura 16 se

puede ver la forma de onda de la tensión aplicada en esta etapa durante un ciclo de experimentación.

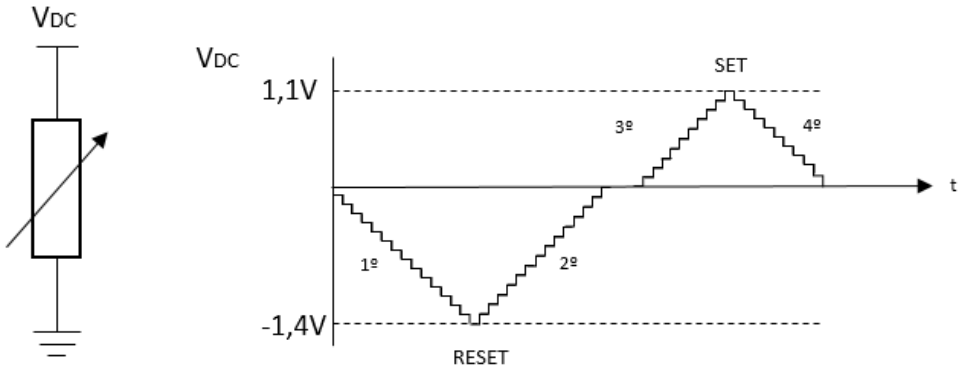


Figura 16. Forma de onda de un ciclo en continua aplicada entre los terminales de una RRAM. Los números son el orden de aplicación de estas rampas y están relacionados con los números de la Figura 17

La operación de *reset* consiste en aplicar una tensión negativa en rampa desde 0V hasta -1,4V de forma que la RRAM conmuta de estado resistivo de LRS a HRS. Cuando se llega a -1,4V entonces comienza la rampa de subida desde -1,4V hasta 0V y aquí es donde termina la operación de *reset*. Durante muy poco tiempo, no se aplica tensión entre los terminales, y a continuación se aumenta la tensión de forma gradual desde 0V hasta 1,1V de manera que la RRAM conmuta de estado resistivo nuevamente de HRS a LRS. Cuando se llega a 1,1V se vuelve a disminuir dicha tensión hasta acabar la operación de *set* en 0V. Con esto se consigue obtener experimentalmente la curva característica I-V real de una RRAM, como se puede ver en la Figura 17, gráficas a) y b). En estas, la operación de *reset* está impresa en rojo, mientras que la operación de *set* lo está en azul.

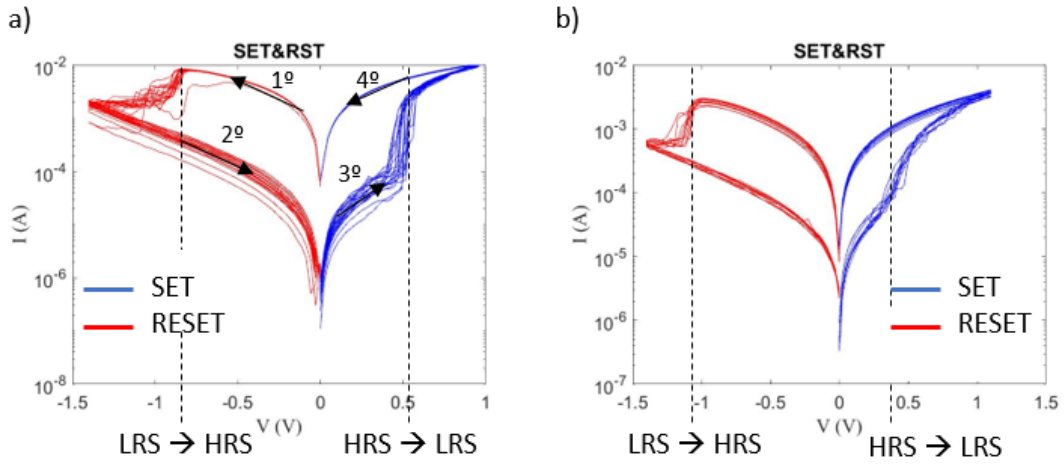


Figura 17. a) Resultado de la experimentación de 50 ciclos en continua de una RRAM. Las rayas verticales en discontinua marcan la V_{SET} y la V_{RESET} en la que se produce la conmutación resistiva. b) 50 ciclos en continua de otra RRAM

Los experimentos realizados, consisten en aplicar 50 ciclos en continua, para ver el comportamiento memristivo de los dispositivos y representar de manera realista la curva característica I-V de una RRAM. En la Figura 17, gráfica a), se aprecia la gran variabilidad que estas presentan cuando están en el estado HRS (parte inferior de las curvas) y la poca que presentan cuando están en el estado LRS (parte superior de las curvas) [21]. Este fenómeno se debe principalmente al CF, que cuando el dispositivo se encuentra en el estado resistivo alto, pequeñas variaciones en la distancia entre el extremo del filamento y el terminal opuesto del dispositivo, provocan grandes variaciones en su resistencia equivalente. A pesar de que es un hecho conocido, no se abarca en este trabajo.

También se puede ver en la Figura 17, gráficas a) y b), el cambio brusco (en unas RRAMs más que en otras) de resistencia que se produce en las operaciones de *set* y de *reset*. Habitualmente, las RRAMs con las que se ha trabajado tienen una V_{RESET} (es la tensión umbral en la que se produce la conmutación de LRS a HRS) de entre -0,7V y -1,1V. Por otra parte, la V_{SET} de las RRAMs (es decir, la tensión umbral en la que se produce la conmutación de HRS a LRS) es de entre 0,4V y 0,6V. No confundir la V_{RESET} y la V_{SET} que son las tensiones umbrales de conmutación de estado resistivo, con las tensiones aplicadas en las operaciones de *reset* (normalmente hasta -1,4V) y de *set* (normalmente hasta 1,1V).

Por último, es importante fijarse en la ventana de conmutación de las RRAMs. Esta se define como la diferencia que existe entre el valor de resistencia cuando el dispositivo está en estado de baja resistencia (LRS) y cuando está en estado de alta resistencia (HRS). En los ciclos en continua, la ventana se puede apreciar, por ejemplo en la Figura 17, gráfica a), para un mismo punto de tensión, la diferencia de corriente que es capaz de conducir entre la zona donde pone 1º (en donde se conduce más corriente y por lo tanto la RRAM está en el estado LRS) y la zona donde pone 2º (en donde la corriente que conduce es menor para una misma tensión, y por lo tanto la RRAM está en el estado HRS). Cuanto mayor sea esta ventana, mayor diferencia del valor de resistencia entre los dos estados de la RRAM y, por lo tanto, mejor comportamiento memristivo.

5.2.3. Etapa nº3: Ciclos en pulsos

En esta tercera etapa de preparación, se aplican pulsos a la RRAM de forma que un ciclo consiste en realizar una operación de *reset* y una operación de *set*, junto con lecturas del valor resistivo. En la operación de *reset* se aplica un pulso con una tensión de -1,4V y en la operación de *set* la tensión aplicada es de 1,1V. Los pulsos tienen un ancho de 5ms y las lecturas se realizan entre el *reset* y el *set* (y entre el *set* y el *reset*) aplicando una tensión de lectura (V_{read}) de ±0,1V para conocer el valor resistivo de la RRAM después de haberle aplicado un pulso de escritura. En la Figura 18, se muestra la secuencia de pulsos que se realiza en cada uno de los ciclos de experimentación:

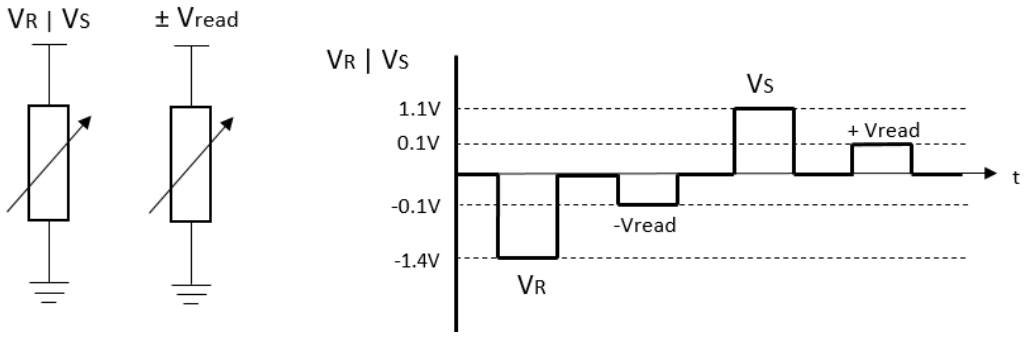


Figura 18. Forma de onda de un ciclo en pulsos aplicados entre los terminales de una RRAM

Esta etapa consiste en aplicar 100 ciclos para mostrar de manera adecuada el comportamiento memristivo que tienen estos dispositivos. La lectura de resistencia de la RRAM, se almacena y se procesa para posteriormente realizar una gráfica en donde se pueden ver los dos estados resistivos, lo que permite apreciar rápidamente la ventana de conmutación. En la Figura 19 se muestra un resultado experimental de esta etapa de preparación:

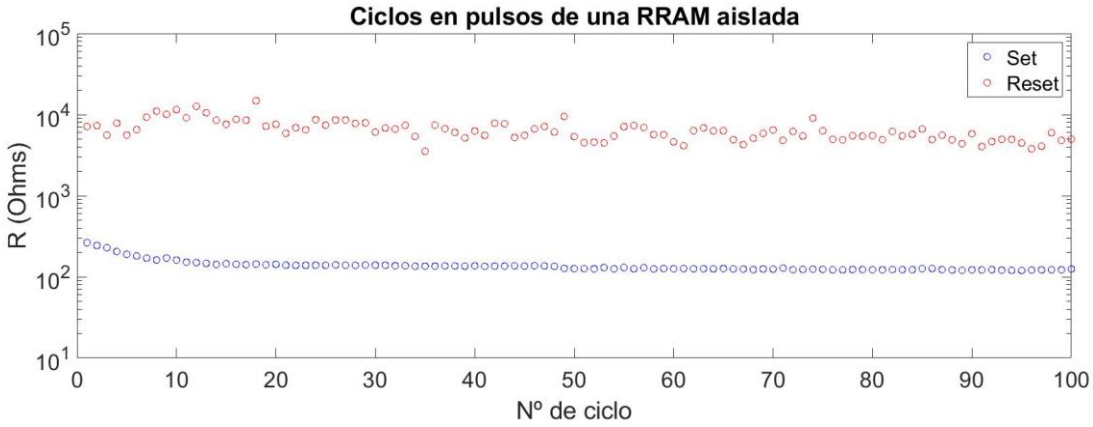


Figura 19. Resistencia equivalente de una RRAM después de aplicar operaciones de set y reset durante 100 ciclos en pulsos

Los puntos rojos representan la lectura de la resistencia de la RRAM cuando se encuentra en el estado HRS después de aplicar una operación de *reset*, mientras que los puntos azules representan la lectura de la resistencia de la RRAM cuando se encuentra en el estado LRS después de aplicar una operación de *set*. Los valores típicos que se han observado de resistencia en ambos estados resistivos son, para el estado HRS, 10kΩ y, para el estado LRS, 200Ω. Al igual que en los ciclos en continua, se observa la gran variabilidad de resistencia ciclo a ciclo que presentan los dispositivos en el estado HRS, en contraposición con la gran uniformidad del valor de resistencia en el LRS. Además, es preciso comentar que la ventana de conmutación resistiva de la RRAM se aprecia de manera mucho más clara cuando se aplican ciclos en pulsos que cuando se realizan ciclos en continua. En el siguiente apartado se explica por qué la ventana de conmutación es una característica tan importante en el desarrollo del presente trabajo.

5.3. Modulación de la resistencia en el estado LRS con la corriente de *compliance*

La ventana de conmutación resistiva de las RRAMs es muy variable y depende, principalmente, de la tecnología con la que han sido desarrolladas. En este trabajo, las ventanas de conmutación de los dispositivos con los que se ha experimentado son de uno o dos órdenes de magnitud.

Es importante comentar el papel fundamental que tiene la corriente de *compliance* que se aplica en la operación de *set* ("Icomps" en adelante) en el valor de la resistencia de la RRAM en el estado LRS. T. Lee et al. también analizan este efecto sobre las RRAMs [22], ya que no solo es importante a nivel de experimentación y preparación, sino que permite modificar la ventana de una RRAM aumentándola o disminuyéndola en función de la Icomps que se aplique. Para demostrar este efecto de modulación del valor resistivo cuando la RRAM está en el estado LRS a través de la Icomps, se realizan dos experimentos que se explican a continuación.

5.3.1. Doble barrido de la corriente de *compliance* en la operación de *set*

El primer experimento se basa en realizar 160 ciclos en pulsos aplicando una tensión en la operación de *set* de 1,1V y una tensión en la operación de *reset* de -1,4V, y en cada ciclo disminuir la Icomps 50µA, en un rango entre 2mA y 50µA. Cuando se alcanzan los 50µA, se incrementa la Icomps 50µA en cada ciclo, desde 50µA hasta 2mA. En la Figura 20, gráficas a) y b), se muestra el resultado del experimento para dos subidas y dos bajadas de Icomps:

a)

b)

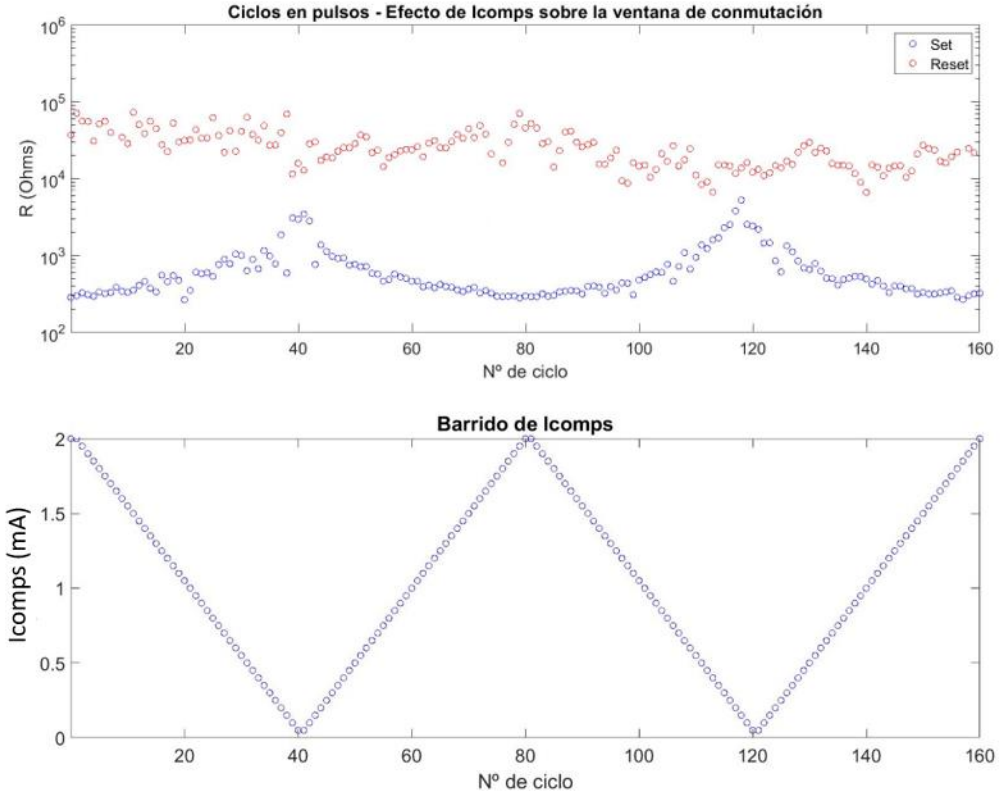


Figura 20. a) Efecto de Icomps en la ventana de conmutación de una RRAM aislada con un doble barrido de corriente. b) Doble barrido de corriente de Icomps

En la Figura 20, gráfica a), se observa la modulación del valor resistivo de la RRAM en el estado LRS (puntos azules) en función del valor de Icomps que se aplique, mientras que en la resistencia en el estado HRS (puntos rojos) no tiene ningún efecto. La resistencia en el estado LRS aumenta si se disminuye la Icomps, mientras que disminuye si se aumenta, por lo que se observa que tiene un efecto significativo en la anchura de la ventana de conmutación.

5.3.2. Barrido ascendente de la Icomps

En la Figura 21 se muestra el resultado de un experimento realizado a otra RRAM, en el cuál se incrementa la Icomps desde 50µA hasta 2mA, aumentándola en cada ciclo 50µA.

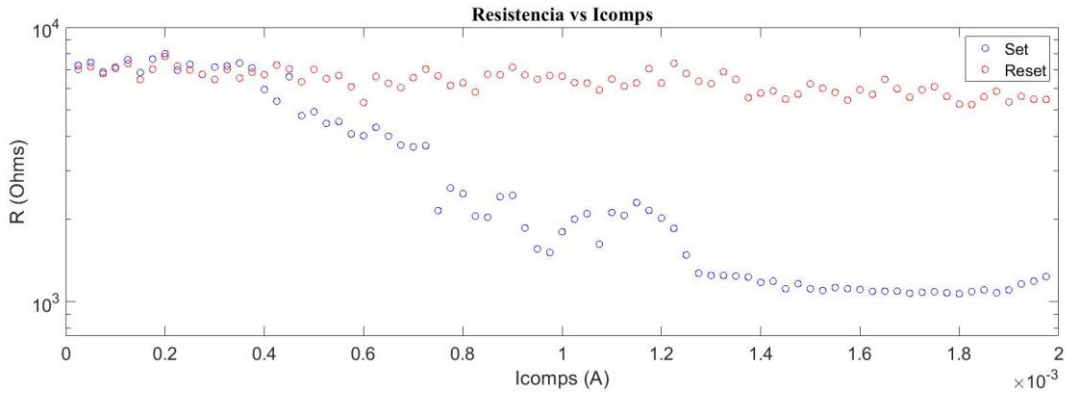


Figura 21. Barrido creciente de la Icomps (eje x) y se ve como cada vez la ventana de conmutación es mayor debido al efecto que se produce sobre la resistencia en el estado LRS

Se representa en el eje Y la lectura del valor de la resistencia de la RRAM en cada ciclo después de una operación de reset (puntos rojos) y de una operación de set (puntos azules), y en el eje X el valor de Icomps. Al principio, la ventana es prácticamente nula (no conmuta) ya que la Icomps es tan pequeña (50µA) que la propia RRAM no cambia su estado resistivo. Conforme se va incrementando la Icomps, el efecto que se presenta sobre la resistencia en el estado LRS es muy notable y la ventana se incrementa hasta que llega tal punto en el que ya no es posible hacerla más grande.

Con estos dos experimentos, en donde se observa empíricamente la dependencia que existe entre la resistencia en el estado LRS de una RRAM y el valor de Icomps que se aplica en la operación de *set*, se fija la base sobre la que se sustentará la celda de memoria enmascarable que se presentará en los capítulos 7 y 8.

6. Experimentación con RRAMs en serie

6.1. Configuración en serie

La configuración en serie de dos RRAMs consiste en conectarlas de forma que el BE de la RRAM superior (R_{top}), esté conectada con el TE de la RRAM inferior (R_{bottom}). En la Figura 22 se puede observar cómo se conectan las RRAMs en serie:

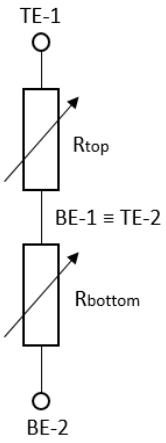


Figura 22. Esquema de la disposición de las RRAMs en serie

Para la realización de los experimentos con dos dispositivos en serie, es necesario haber realizado previamente todas las etapas de preparación que se han explicado en el capítulo anterior de ambas RRAMs por separado (*forming*, ciclos en continua y ciclos en pulsos). Con el *forming* realizado a R_{top} y R_{bottom}, se realizan 50 ciclos en continua a cada una de ellas y se presentan en la Figura 23:

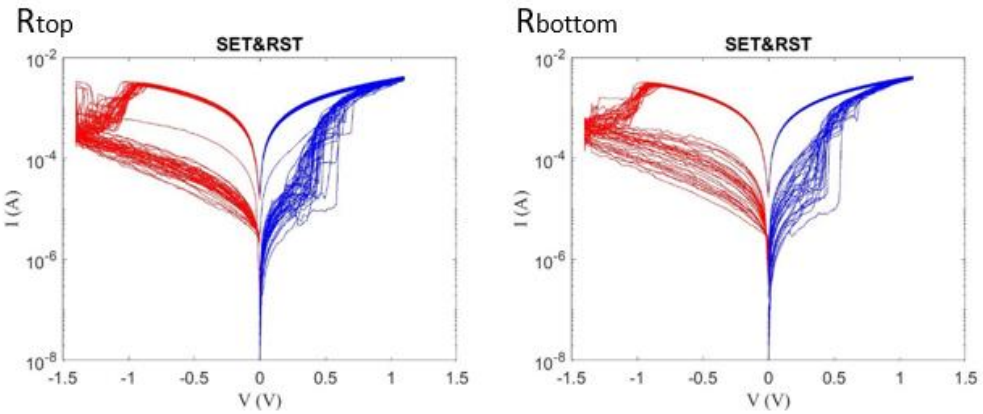


Figura 23. Característica I-V realizando 50 ciclos en continua a R_{top} y R_{bottom} por separado

Una vez que ambas se comportan adecuadamente cuando se aplican 50 ciclos en continua, se procede a aplicar 100 ciclos en pulsos a cada una de las RRAMs por separado con las mismas características que se ha comentado para esta prueba en el capítulo anterior, sin limitación de corriente durante la operación de *set*.

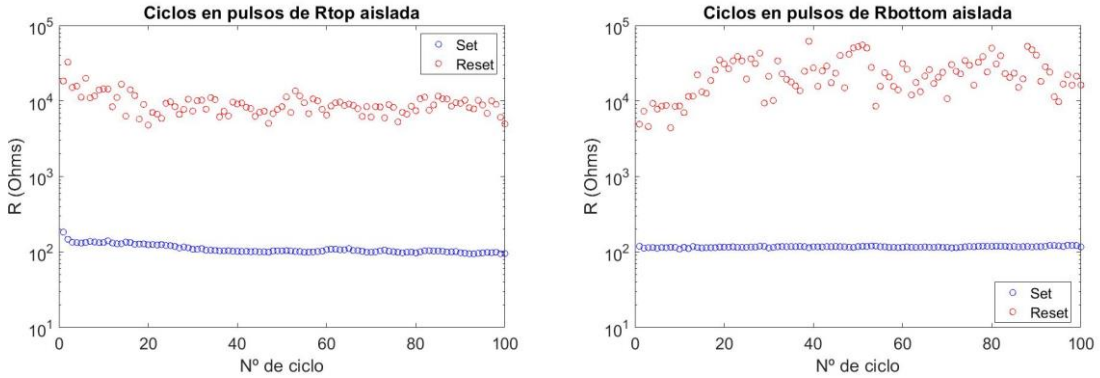


Figura 24. 100 ciclos en pulsos a cada RRAM por separado para comprobar que la ventana es suficiente y su comportamiento memristivo es el deseado

Una vez que se ha comprobado que las RRAMs tienen un comportamiento memristivo correcto, se procede a experimentar con estas en serie.

La experimentación con los dispositivos en serie consiste en ciclos en donde se aplican pulsos de forma similar a la etapa nº3 de los dispositivos aislados, pero con los dispositivos configurados en serie como en la Figura 22. En la operación de *reset* en serie se aplica una tensión de -1,4V mientras que en la operación de *set* en serie se aplica una tensión de 1,1V. Entre el *set* y el *reset* (y entre el *reset* y el *set*), se hace una lectura por separado del valor resistivo de cada RRAM con una tensión de lectura (V_{read}) de ±0,1V. Los valores de tensión tanto para lo operación de *set* en serie como para la de *reset* en serie son variables, y en ocasiones hay que incrementarlos. En la operación de *set* se puede incrementar hasta 1,3V y en la operación de *reset* hasta -1,7V. Este incremento en las tensiones de operación en serie, se debe al divisor resistivo formado por las dos RRAMs, que puede darse el caso de que tengan un valor resistivo semejante, caiga una tensión en las dos parecida y como consecuencia, ninguna de ellas conmute de estado resistivo ya que no se alcanzan las tensiones umbrales (V_{SET}, V_{RESET}) de ninguna de las dos RRAMs. En la Figura 25 se muestran los pulsos que se realizan en los terminales de las RRAMs en serie en un ciclo de experimentación.

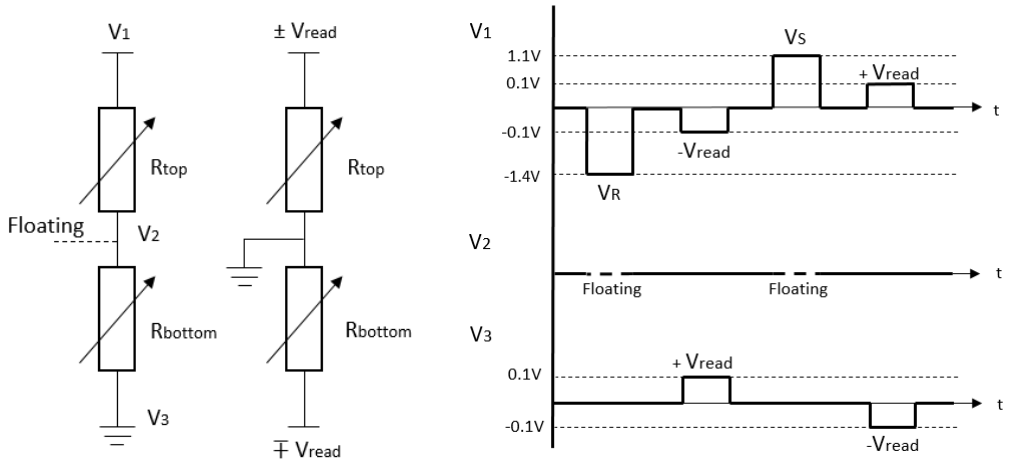


Figura 25. Las operaciones de set y de reset, se realizan colocando las dos RRAMs en serie. Las operaciones de lectura se realizan a cada RRAM por separado

Cuando se realiza la lectura del estado resistivo de cada RRAM por separado, el terminal común de las dos RRAMs (V_2) se conecta a tierra, mientras que cuando se realiza una operación de *set* o de *reset* en serie, V_2 se pone flotando (*"Floating"*) de forma que las dos RRAMs quedan configuradas en serie.

En la Figura 26, gráfica a), se muestra el resultado de experimentación para la operación de *set* en serie. Los puntos azules representan la resistencia de R_{top} cuando se le aplica un pulso de lectura después de realizar una operación de *set* en serie, y los puntos rojos representan la resistencia de R_{bottom} cuando se le aplica un pulso de lectura después de realizar la misma operación. En la Figura 26, gráfica b), se muestra el resultado de experimentación para la operación de *reset* en serie. Los puntos azules representan la resistencia de R_{top} cuando se le aplica un pulso de lectura después de realizar una operación de *reset* en serie, y los puntos rojos representan la resistencia de R_{bottom} cuando se le aplica un pulso de lectura después de realizar la misma operación.

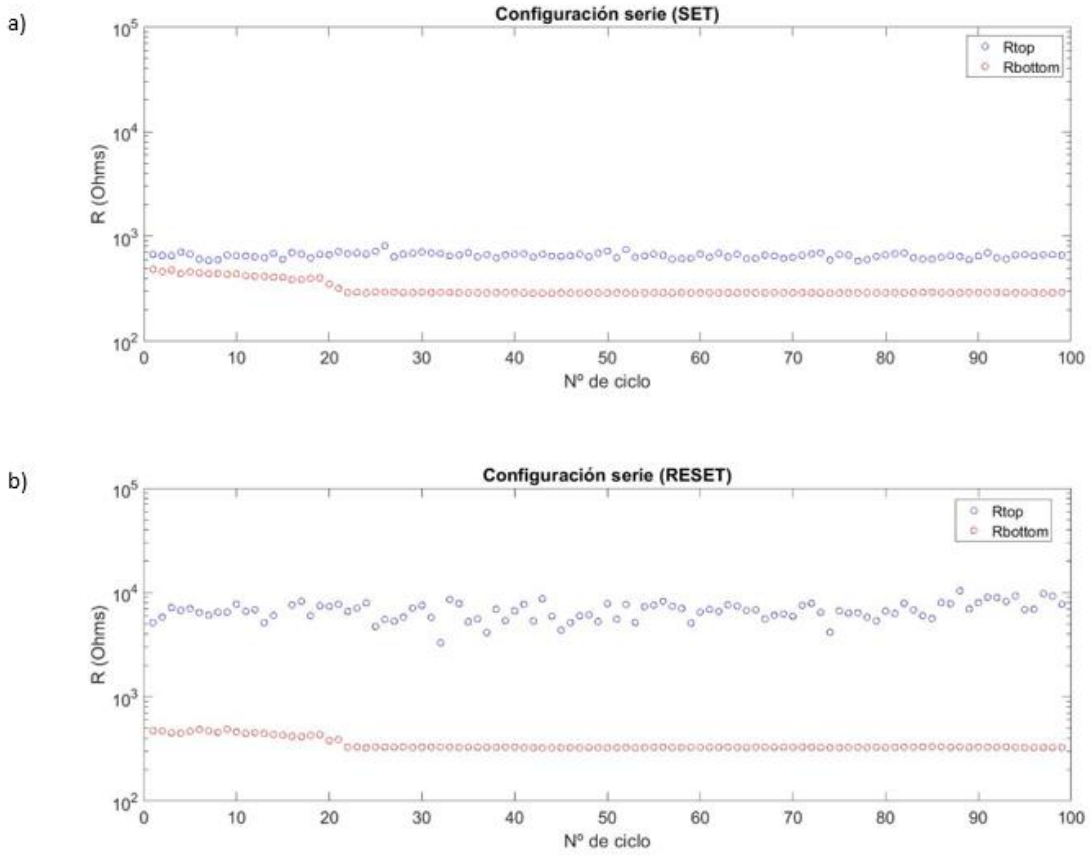


Figura 26. a) Operación de set efectuada sobre las RRAMs en serie. Se puede observar claramente como el valor resistivo en LRS de R_{top} es mayor que el de R_{bottom}. b) Operación de reset efectuada sobre las RRAMs en serie. R_{top} conmuta de LRS a HRS mientras que R_{bottom} se mantiene en el estado LRS

La experimentación con dispositivos en serie se llevó a cabo con 25 parejas, de las cuáles 12 dejaron de funcionar durante la experimentación. En el Anexo B se puede encontrar las figuras para las 13 parejas que funcionaron, tanto para la operación de set como para la de reset. Se observa que, en todas las parejas, siempre hay una que conmuta de estado de LRS a HRS cuando se realiza la operación de reset en serie, mientras que la otra se queda en el estado LRS. En la Tabla 1 se indica qué RRAM de la pareja es la que ha conmutado, R_{top} o R_{bottom}, al menos durante 50 ciclos:

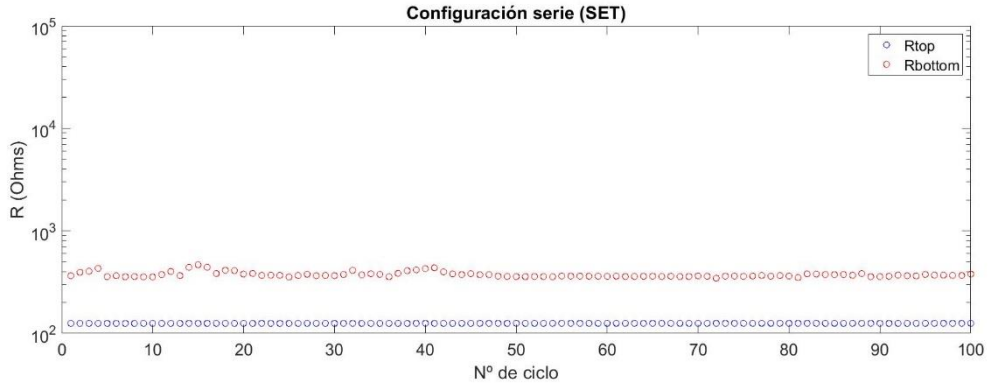
Nº de la pareja	Cuál ha conmutado
1	R_{top}
2	R_{top}
3	R_{top}
4	R_{bottom}
5	R_{top}
6	R_{bottom}
7	R_{top}
8	R_{bottom}
9	R_{bottom}
10	R_{top}
11	R_{bottom}
12	R_{bottom}
13	R_{top}

Tabla 1. Identificación de las parejas y cuál de las dos RRAMs de la pareja ha conmutado en serie

De estas experimentaciones, se puede afirmar lo que se advierte en la publicación [1]:

- Colocando dos RRAMs en serie, siempre conmuta de LRS a HRS en la operación de *reset* en serie, aquella que tiene un valor resistivo en el estado LRS mayor. En la Figura 27, gráficas a) y b), se aprecia como ahora la RRAM que conmuta es la R_{bottom}, ya que su resistencia en LRS es mayor que la de R_{top}. Por ello, es indistinta la posición de las RRAMs en la configuración serie, ya que la conmutación de R_{top} o R_{bottom} depende del valor resistivo en el estado LRS.

a)



b)

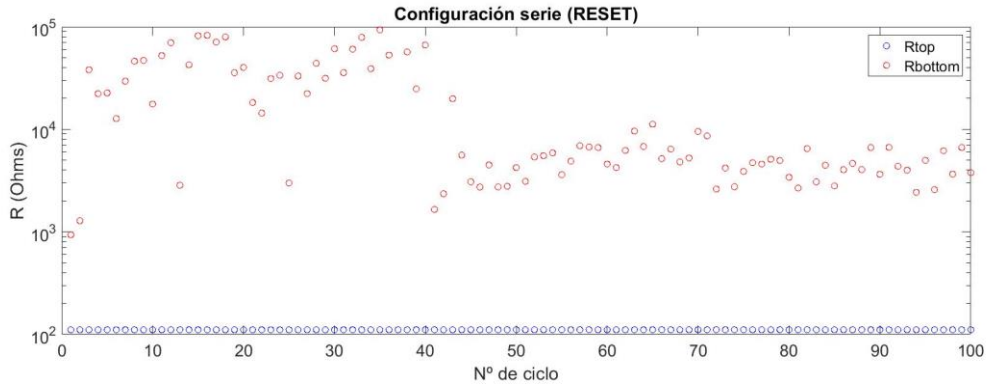


Figura 27. a) Operación de set efectuada sobre las RRAMs en serie. A diferencia de la Figura 26, la R_{bottom} presenta un valor resistivo en LRS mayor que la R_{top}. b) Operación de reset efectuada sobre las RRAMs en serie. Como ahora es R_{bottom} quién presenta un valor resistivo en LRS mayor que R_{top}, es la que conmuta de la pareja durante todos los ciclos de experimentación

- En una misma pareja de RRAMs, dados N ciclos, siempre conmuta la misma.

Estas observaciones, además de haber sido demostradas experimentalmente, también han sido modeladas teóricamente. Suponiendo que las RRAMs están en el estado LRS y se aplica una operación de *reset* en serie, se obtiene lo siguiente:

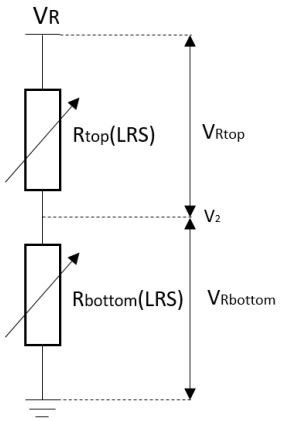


Figura 28. Esquema del modelo teórico de las RRAMs en serie cuando se encuentran en el estado LRS

De la Figura 28 se deducen las ecuaciones 3 y 4:

$$V_{Rtop} = V_{reset} - V_2 = V_{reset} \frac{R_{top}(LRS)}{R_{top}(LRS) + R_{bottom}(LRS)} \quad \text{(Ec.3)}$$

$$V_{Rbottom} = V_2 = V_{reset} \frac{R_{bottom}(LRS)}{R_{top}(LRS) + R_{bottom}(LRS)} \quad \text{(Ec.4)}$$

Por lo tanto, teóricamente y suponiendo un valor constante de resistencia en el estado LRS en ambas RRAMS de ciclo en ciclo (lo cual es coherente con los resultados experimentales), se pueden deducir las gráficas a), b) y c) de la Figura 29 para cualquier pareja de RRAMs en serie, poniendo el valor resistivo de R_{top} en función de R_{bottom}. Se representa la caída de tensión en cada RRAM (eje Y) con respecto a la tensión aplicada en la operación de *reset* en serie (eje X).

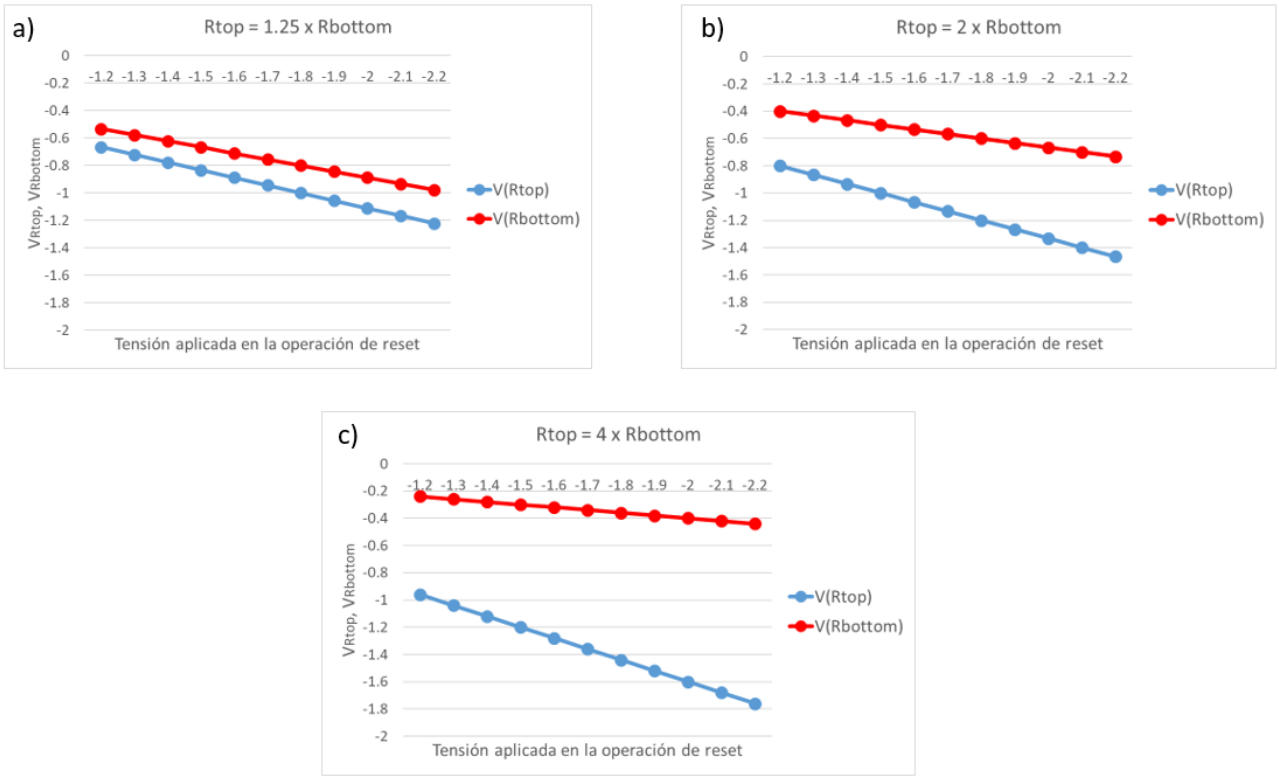


Figura 29. a) Resistencia en LRS de R_{top} 1,25 veces mayor que la de R_{bottom}. b) Resistencia en LRS de R_{top} el doble que la de R_{bottom}. c) Resistencia en LRS de R_{top} cuatro veces mayor que la de R_{bottom}

De estas tres gráficas, se puede concluir que, cuanto mayor sea la relación entre las resistencias en el estado LRS de una RRAM respecto de la otra, mayor caída de tensión entre los terminales de la RRAM con la resistencia más alta en el estado LRS para una misma tensión de operación de *reset* en serie.

Por lo tanto, durante la operación de *reset* en serie, la RRAM con mayor resistencia en el estado LRS antes alcanzará la tensión umbral V_{RESET} necesaria para conmutar de LRS a HRS. Este modelo teórico confirma las experimentaciones en las que siempre conmuta aquella que tiene mayor resistencia en el estado LRS. Además, se deduce de las gráficas a), b) y c), que la RRAM que no conmuta de una pareja, siempre estará en el estado LRS durante todos los ciclos de experimentación, ya que la caída de tensión entre sus terminales no será suficiente como para alcanzar la tensión umbral V_{RESET} necesaria (alrededor de -0,7V) para realizar la conmutación.

7. Concepto de enmascaramiento y funcionalidad de la celda de memoria

En las memorias no volátiles, los datos están almacenados en forma binaria (‘1’ o ‘0’). Como ya se ha comentado, las RRAMs pueden trabajar de esta forma, conmutando entre los estados LRS y HRS. Por lo tanto, se diseña una celda de memoria basada en dos RRAMs en serie cuyo funcionamiento presentará tres posibles estados:

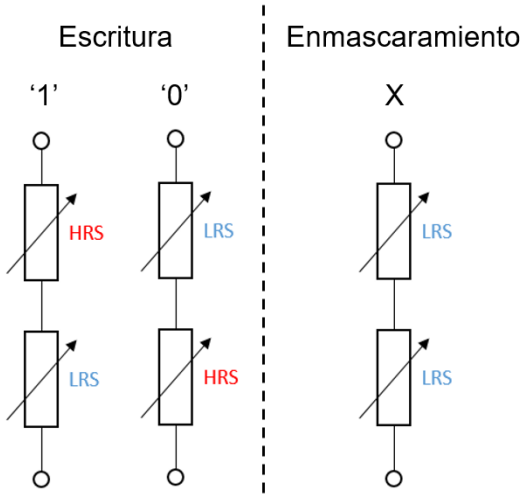


Figura 30. Estados posibles de la celda de memoria

En la operación de escritura se podrá guardar un ‘1’ en caso de que la R_{top} sea la que conmute de LRS a HRS o un ‘0’ en caso de que sea R_{bottom} la que conmute de estado resistivo.

El tercer estado de la celda de memoria es ‘X’, que se alcanza en la operación de enmascaramiento de la celda y en el cuál las dos RRAMs se encuentran en estado LRS. El concepto de enmascaramiento se basa en tener los dos dispositivos en serie con el valor de resistencia lo más parecido posible (idealmente el mismo) para que un atacante que únicamente pueda medir su valor, no sea capaz de determinar de manera fiable cuál de las dos RRAMs tendrá una resistencia mayor en el estado LRS y, por lo tanto, no pueda predecir cuál será el dato almacenado.

El funcionamiento de la celda de memoria enmascarable es el siguiente:

- Caso 1: con la celda de memoria utilizada por un usuario legitimado se pueden realizar operaciones de escritura (operación de *reset* y *set* a cada dispositivo por separado), operaciones de lectura (operación de *reset* en serie) y operaciones de enmascaramiento (operación de *set* en serie). No confundir la operación de lectura de la celda de memoria, que se realiza con una operación de *reset* en serie, con la lectura de una RRAM, que se realiza para conocer su valor resistivo y se hace a cada RRAM

por separado aplicando una tensión pequeña. En la operación de escritura en el *set* por separado, se hace circular una Icomps diferente por cada RRAM, modulando el valor de resistencia en el estado LRS de los dispositivos. Por lo tanto, habrá dos niveles de Icomps:

- IcompsL: es el valor de la corriente de *compliance* de la operación de *set* menor, por lo que la resistencia en el estado LRS será mayor. (Ver Figura 21)
- IcompsH: es el valor de la corriente de *compliance* de la operación de *set* mayor, por lo que la resistencia en el estado LRS será menor.

En la Figura 31 y Figura 32, se pone un ejemplo de operación para escribir y guardar un '1' o un '0' respectivamente en la celda de memoria:

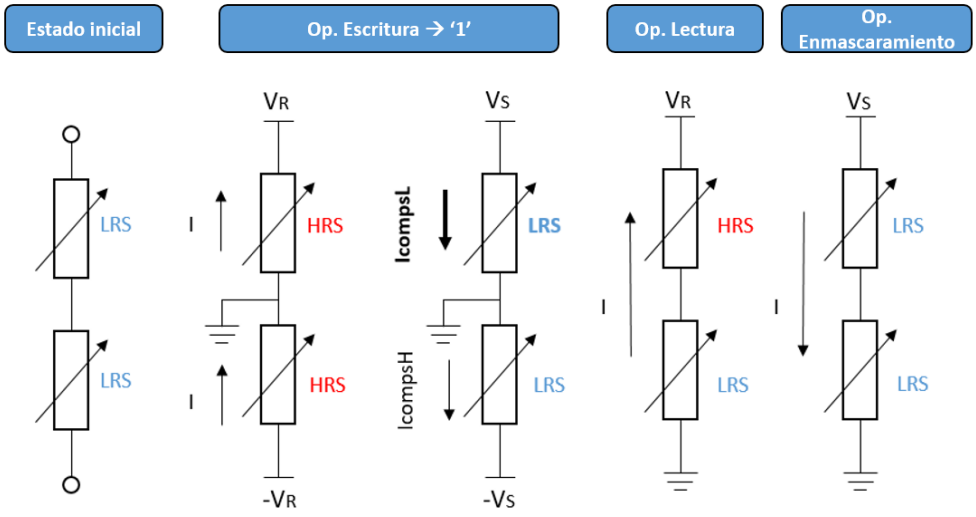


Figura 31. Escritura, lectura y enmascaramiento de un '1' en la celda de memoria

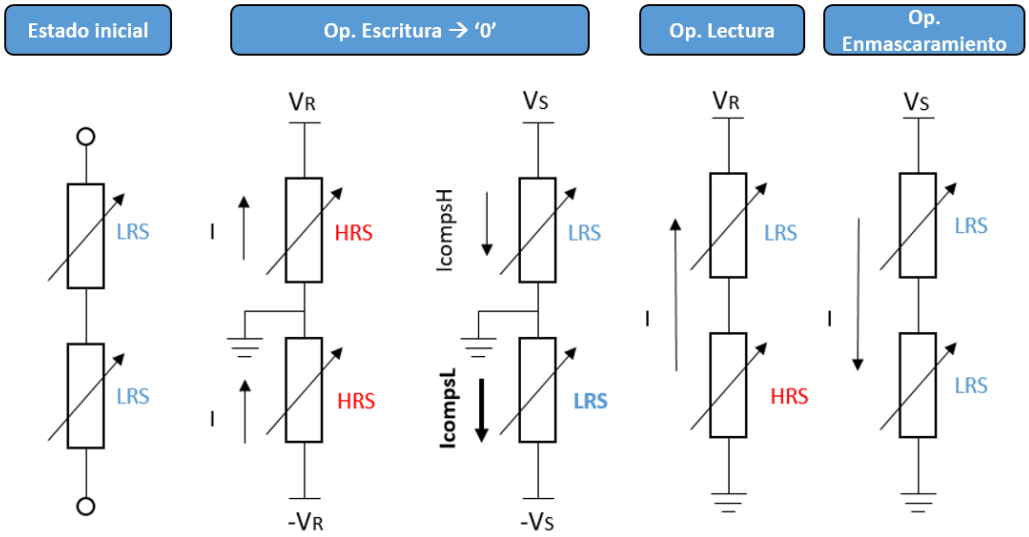


Figura 32. Escritura, lectura y enmascaramiento de un '0' en la celda de memoria

- Caso 2: con la celda de memoria medida por un atacante y sin fuente de alimentación conectada, éste no va a poder realizar ninguna operación sobre las RRAMs, únicamente podrá medir el valor resistivo de cada una por separado. Por lo tanto, si el usuario legitimado realiza el enmascaramiento antes de dejar las RRAMs sin alimentación, lo que el atacante leerá será el valor de la resistencia en el estado LRS y, en consecuencia, no podrá detectar de forma fiable cuál de las dos, si R_{top} o R_{bottom}, es la que va a conmutar en la operación de lectura. El dato estará protegido.

El diseño y la viabilidad de la celda de memoria se basa en las observaciones que se han ido verificando a lo largo de este trabajo:

- Con dispositivos aislados: existe un efecto directo de la Icomps en la ventana de conmutación de la RRAM, pudiendo incrementar o disminuir el valor de la resistencia de la RRAM en el estado LRS.
- Con dispositivos en serie: Durante todos los ciclos de experimentación conmuta la RRAM cuya resistencia es mayor en el estado LRS, indistintamente de si es R_{top} o R_{bottom}. [1]

7.1. Experimento nº1: Forzar la conmutación de una RRAM

El objetivo de este experimento es demostrar la capacidad de modular la resistencia de las RRAMs en el estado LRS para forzar la conmutación de una de las dos cuando se configuran en serie. Se establece una variable aleatoria *"x"* para determinar a cuál de las dos RRAMs afectará la IcompsL y, por consiguiente, la operación de escritura de un '1' o un '0' será aleatoria en cada ciclo. Los dos niveles de *compliance* diferentes (IcompsL e IcompsH), dan lugar a sendos niveles de resistencia de cada RRAM en el estado LRS:

- Nivel de resistencia alto en el estado LRS: cuando se aplica un valor de IcompsL de 500µA.
- Nivel de resistencia bajo en el estado LRS: cuando se aplica un valor de IcompsH de 2mA.

Los valores de IcompsL e IcompsH son escogidos de manera intuitiva al comienzo del experimento, y posteriormente se van refinando en función de los resultados obtenidos. Esto es un proceso iterativo en donde se busca satisfacer un compromiso entre la igualdad del valor de resistencia en el estado LRS (una de las premisas del concepto de enmascaramiento) y que la RRAM a la que se le ha aplicado la IcompsL sea la que conmute en la operación de lectura.

En la Figura 33 se muestra el diagrama de flujo del programa utilizado para hacer el proceso de escritura, lectura y enmascaramiento en cada ciclo de experimentación:

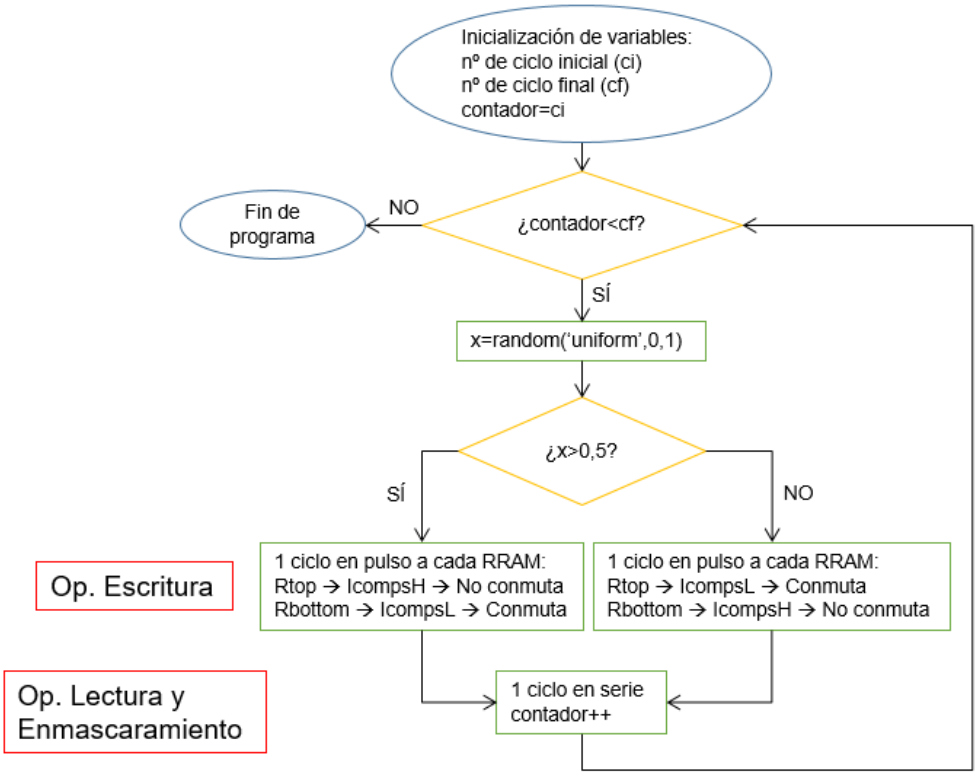


Figura 33. Diagrama de flujo del programa realizado en Matlab para realizar el experimento nº1

Los resultados de una de las parejas ha sido el siguiente. En primer lugar, se muestran los ciclos en pulsos de cada RRAM por separado, es decir, la operación de escritura en la celda que consta de una operación de *reset* y una operación de *set* a cada RRAM, poniendo el nodo del medio a tierra, como se puede ver en la Figura 34:

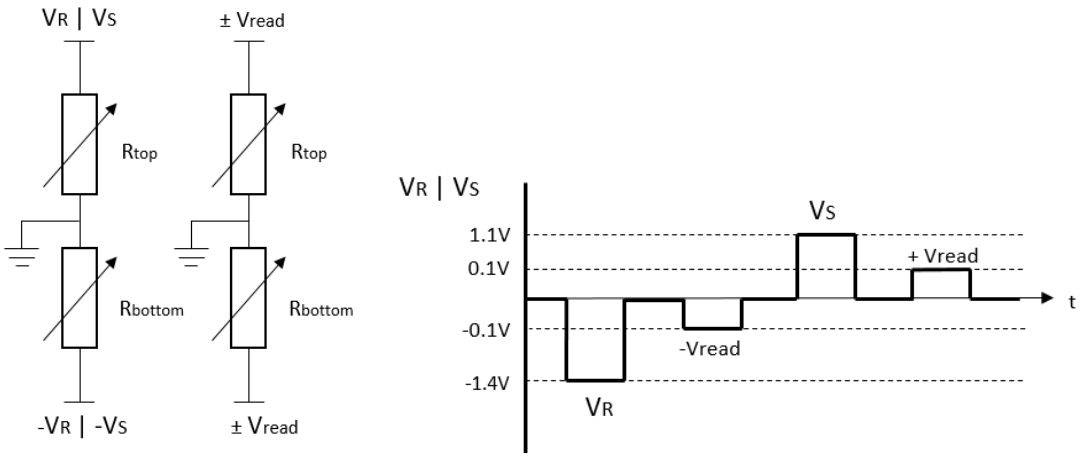


Figura 34. Forma de onda en la operación de escritura de cada RRAM por separado

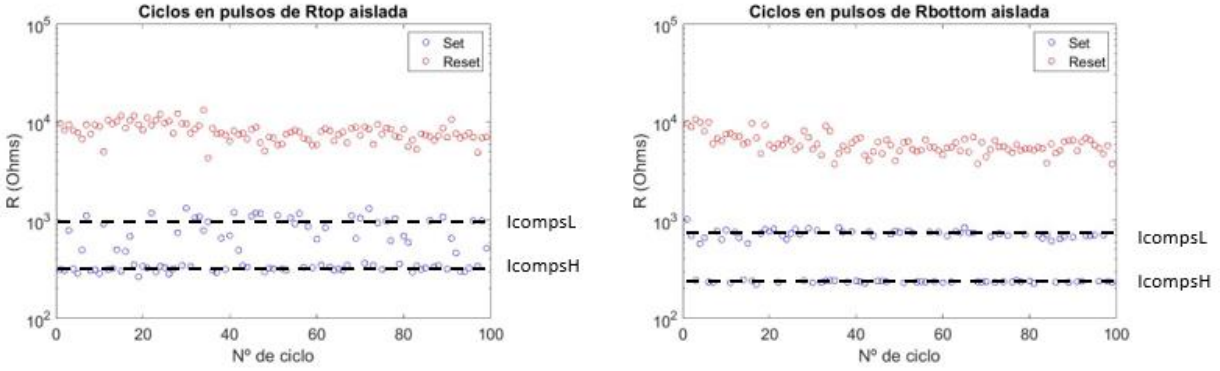


Figura 35. Ciclos en pulsos de cada RRAM por separado. Operación de escritura

En la Figura 35 se puede observar que tanto la R_{top} como la R_{bottom} presentan tres niveles resistivos, dos de ellos marcados con una línea de guiones correspondientes a los dos niveles resistivos en el estado LRS, y el otro en rojo correspondiente al estado HRS. El nivel resistivo más alto del estado LRS corresponde a los ciclos en los que la RRAM ha sido afectada por la IcompsL. El nivel resistivo más bajo del estado LRS, corresponde a los ciclos en los que la RRAM ha sido afectada por la IcompsH, presentando una ventana mayor. Después de cada ciclo de escritura que se realiza a las dos RRAMs por separado, se realiza seguidamente un ciclo en serie y se comprueba que la RRAM que ha conmutado ha sido la afectada por la IcompsL. En la Figura 36 se observa que se realiza, en primer lugar, un *reset* en serie, que es la operación de lectura de la celda, a continuación se lee el valor resistivo de cada RRAM de forma aislada, después se realiza un *set* en serie, que es la operación de enmascaramiento, y por último se vuelven a leer los valores resistivos de cada RRAM de forma aislada. En la Figura 37 se muestran los resultados de las lecturas de los valores resistivos de cada RRAM, tanto en la operación de lectura de la celda (operación de *reset* en serie) como en la operación de enmascaramiento (operación de *set* en serie):

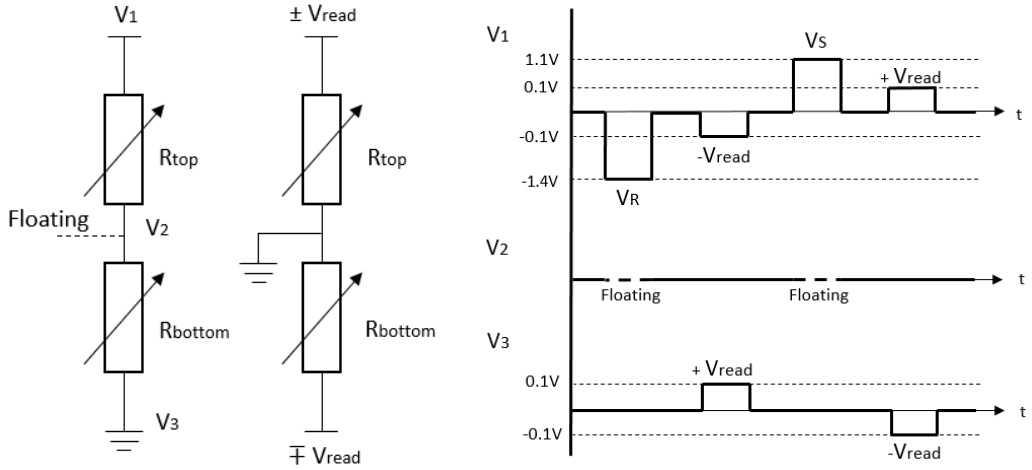


Figura 36. Operación de lectura (reset) y operación de enmascaramiento (set) que se realiza con los dispositivos en serie

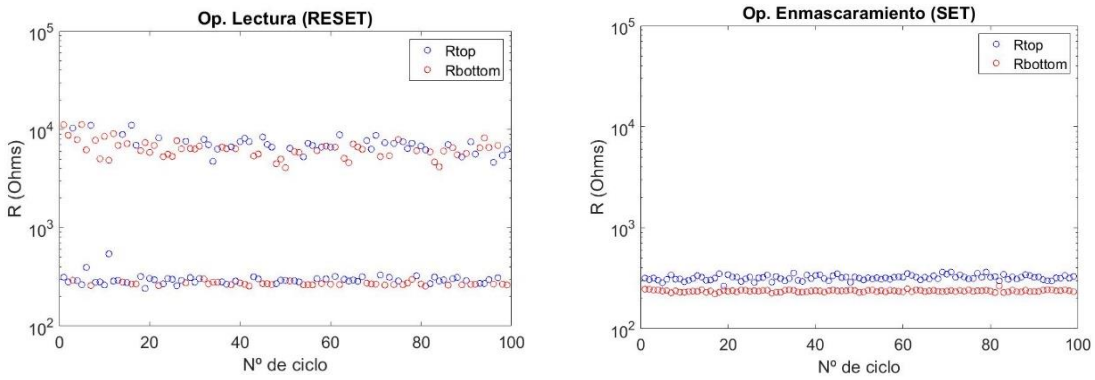


Figura 37. 100 ciclos en pulsos con las RRAMs conectadas en serie. En la operación de lectura se realiza un pulso de reset en serie, mientras que en la operación de enmascaramiento se realiza un pulso de set en serie

En la operación de lectura, se observa que la RRAM que conmuta cambia de forma aleatoria según el valor de la variable: *"x<0,5"* (conmuta R_{top}) o *"x>0,5"* (conmuta R_{bottom}).

En la Figura 38, se presentan estos datos de manera más visual. Cada punto azul representa un ciclo en el que R_{top} está en el estado HRS cuando ha sido afectada por la IcompsL respecto a R_{bottom} que mantiene el estado LRS, y cada punto de color rojo representa un ciclo en el que R_{bottom} está en el estado HRS cuando ha sido afectada por IcompsL respecto a R_{top} que se queda en su estado LRS. Los puntos azules son los ciclos en los que se ha escrito un '1' en la operación de escritura, y los puntos rojos representan los ciclos en los que se ha escrito un '0' en la operación de escritura. Por tanto, las lecturas de la celda son correctas si todos los puntos azules se encuentran en el cuadrante superior izquierdo y todos los puntos rojos en el cuadrante inferior derecho. Por ejemplo, si alguno de los puntos azules se encuentra en la nube de puntos rojos, significa que se había escrito un '1' y sin embargo se ha leído un '0', y viceversa.

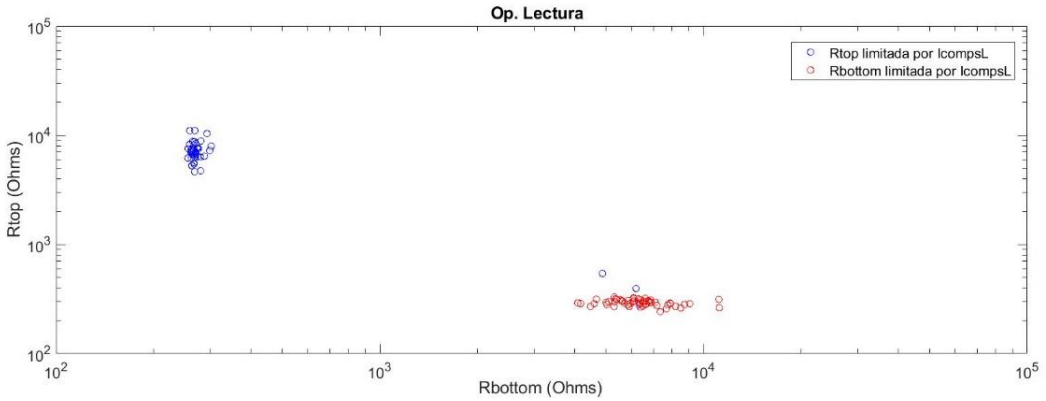


Figura 38. Operación de lectura de la celda de memoria. En azul se muestra el valor de R_{top} cuando ha sido limitada por IcompsL y en rojo se muestra el valor de R_{bottom} cuando ha sido limitada por IcompsL

Se considera que el porcentaje de escritura y lectura es correcto al 100% si todos los puntos azules y rojos están juntos respectivamente. El porcentaje de escrituras y lecturas correctas para esta pareja de RRAMs es del 97%. La Tabla 2 muestra los resultados obtenidos para

siete parejas de RRAMs a las que se ha aplicado el mismo proceso de escritura, lectura y enmascaramiento con sus respectivos porcentajes de lecturas correctas. En el Anexo C se pueden ver las figuras con la operación de lectura de cada pareja.

Pareja nº	Nº de lecturas correctas	Nº de lecturas incorrectas	Porcentaje de lecturas correctas
1	98	2	98%
2	100	0	100%
3	97	3	97%
4	98	2	98%
5	98	2	98%
6	100	0	100%
7	100	0	100%

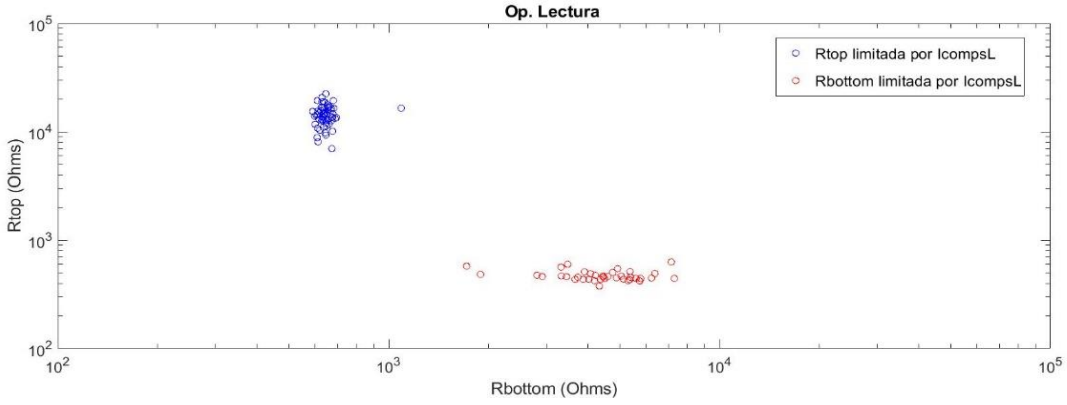
Tabla 2. Parejas de RRAMs a las que se ha forzado la conmutación de una de ellas y el porcentaje de lecturas correctas

Los resultados obtenidos demuestran que existe un mínimo riesgo de fallos en la operación de escritura y lectura de la celda de memoria.

La relación entre la IcompsL (500µA) y la IcompsH (2mA), se varía durante los experimentos para encontrar una relación óptima que permita realizar un buen enmascaramiento y a su vez, conseguir un porcentaje alto de escrituras y lecturas correctas. Después de múltiples experimentos, se observa que las de corrientes de *compliance* óptimas son 250 µA para IcompsL y 1mA para IcompsH, ya que dan lugar a un enmascaramiento de las resistencias en el estado LRS notablemente mejor.

En la Figura 39, gráficas a) y b), se representan las operaciones de lectura y enmascaramiento para una nueva pareja:

a)



b)

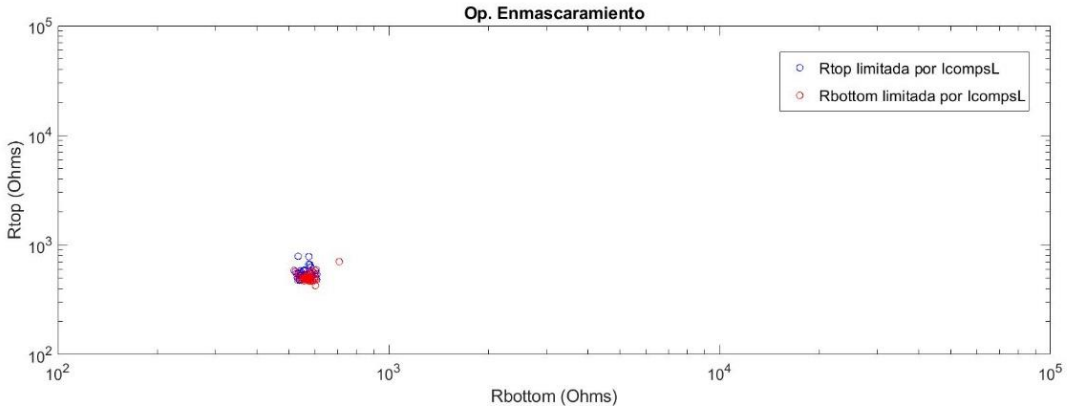
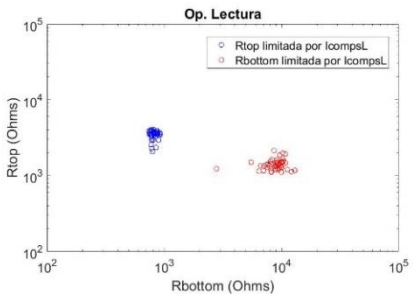
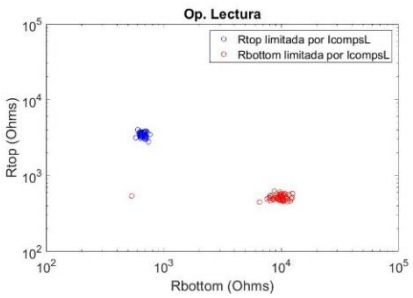
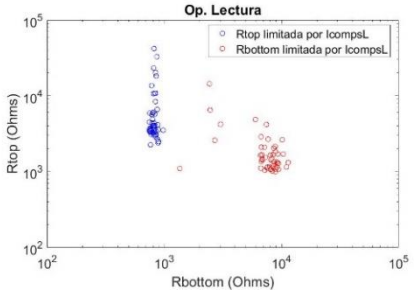
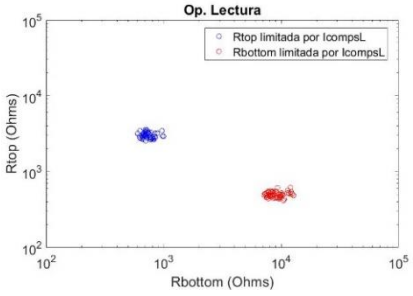
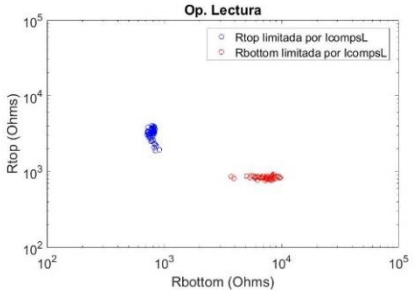
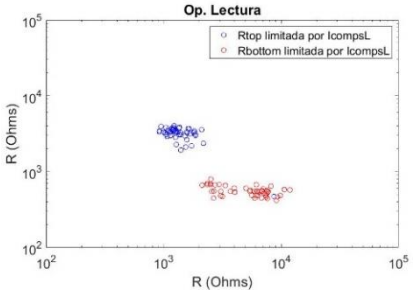


Figura 39. a) Operación de lectura de la celda de memoria. b) Operación de enmascaramiento

Se observa como en la operación de enmascaramiento de las RRAMs (Figura 39, gráfica b)), aparece una nube de puntos azules y rojos superpuestos, que indica que ambas RRAMs tienen un valor muy similar de resistencia en el estado LRS. Esto es un ejemplo de buen enmascaramiento muy difícil de revertir por un atacante.

Con la nueva relación de corrientes entre la IcompsL (250 µA) y la IcompsH (1mA), se realiza un nuevo experimento para otra pareja configurada en serie. En él, se demuestra que las RRAMs no son afectadas por el sentido del barrido, es decir, si la IcompsL se incrementa o se disminuye en la experimentación, ya que la tasa de fallos no depende de esta limitación como se puede ver en la Tabla 3. Para llevar a cabo este experimento, se realizan dos vueltas. En la primera vuelta, se incrementa la IcompsL desde 125µA hasta 1mA. Cuando se llega a este punto, comienza la segunda vuelta, en la que se disminuye la IcompsL desde 1mA hasta 125µA. La IcompsH durante todo el experimento se mantiene en 1mA. La tasa de fallos se realiza contabilizando los puntos azules y/o rojos que no están con los de su color, que es cuando ha habido un error en la escritura y posterior lectura. En la Tabla 3 se pueden ver los resultados obtenidos:

Icompsl (µA)	Resultado 1ª vuelta	Resultado 2ª vuelta	Tasa de fallos	
			1ª	2ª
125			0%	1%
250			3%	0%
500			0%	1%

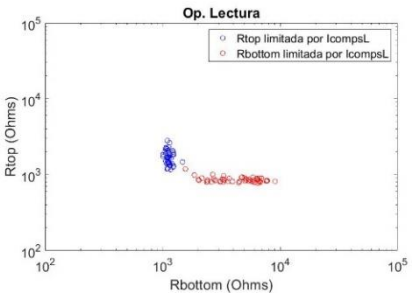
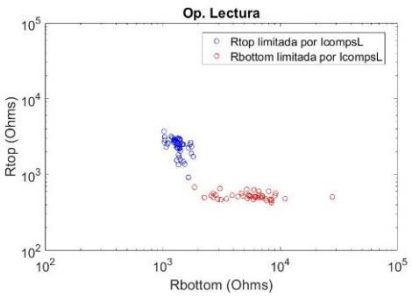
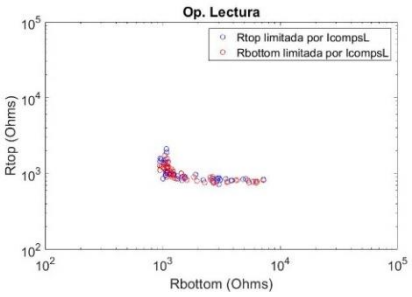
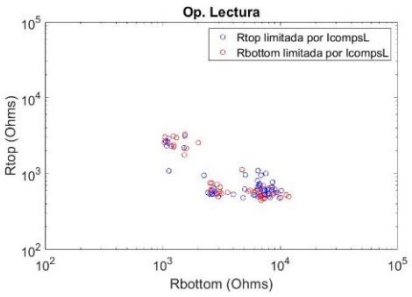
750			2%	5%
1000			50 %	60 %

Tabla 3. Resultados de la experimentación con RRAMs en serie aplicando una operación de lectura y realizando un barrido de la IcompsL primero ascendente, y luego descendente

Se puede observar que la tasa de fallos puede ser mayor o menor, independientemente de si es en la 1ª o en la 2ª vuelta, por lo que no afecta el sentido del barrido de IcompsL en la tasa de fallos de escritura y lectura de la celda.

En el último caso específico en el que IcompsL es igual a la IcompsH (1mA), y por lo tanto no se limita ninguna de las dos RRAMs de la pareja, el factor determinante para que conmute una u otra es la tensión de operación de *reset* en serie que se aplica. En la primera vuelta se aplica una tensión de operación de *reset* de -1,4V que es insuficiente para que conmute cualquiera de las dos como se ve en la imagen de la Tabla 3 (tanto R_{top} como R_{bottom} están en LRS). Sin embargo, en la segunda vuelta únicamente para este caso, se aplica una tensión de *reset* de -1,7V y se puede apreciar como mayoritariamente la RRAM que conmuta es R_{bottom}. Esto se debe a que R_{bottom} tiene una resistencia en el estado LRS mayor y, por lo tanto, es la que tiende a conmutar cuando no se limita la Icomps a ninguna de las dos.

7.2. Experimento nº2: Persistencia del dato escrito en la celda de memoria

Una vez que se ha demostrado que es posible forzar la conmutación de una RRAM limitando la Icomps en la operación de escritura, se realiza un nuevo experimento con las RRAMs en serie para validar que este efecto es persistente durante varios ciclos. De esta forma, se pretende demostrar que las RRAMs pueden servir como celdas de memorias no volátiles seguras.

El experimento empieza, como en el caso anterior, realizando una operación de escritura a cada RRAM por separado mediante una operación de *reset* y de *set* independientes, en las que se impone a una de ellas, en la operación de *set,* la IcompsL. Seguidamente se aplican cinco ciclos de lectura (operación de *reset* en serie) y enmascaramiento (operación de *set* en serie).

En la Figura 40Figura 40 se presenta el diagrama de flujo del programa realizado, que es similar al utilizado en el apartado anterior, aunque ahora se incluyen los cinco ciclos en serie de lectura y enmascaramiento por cada ciclo de escritura:

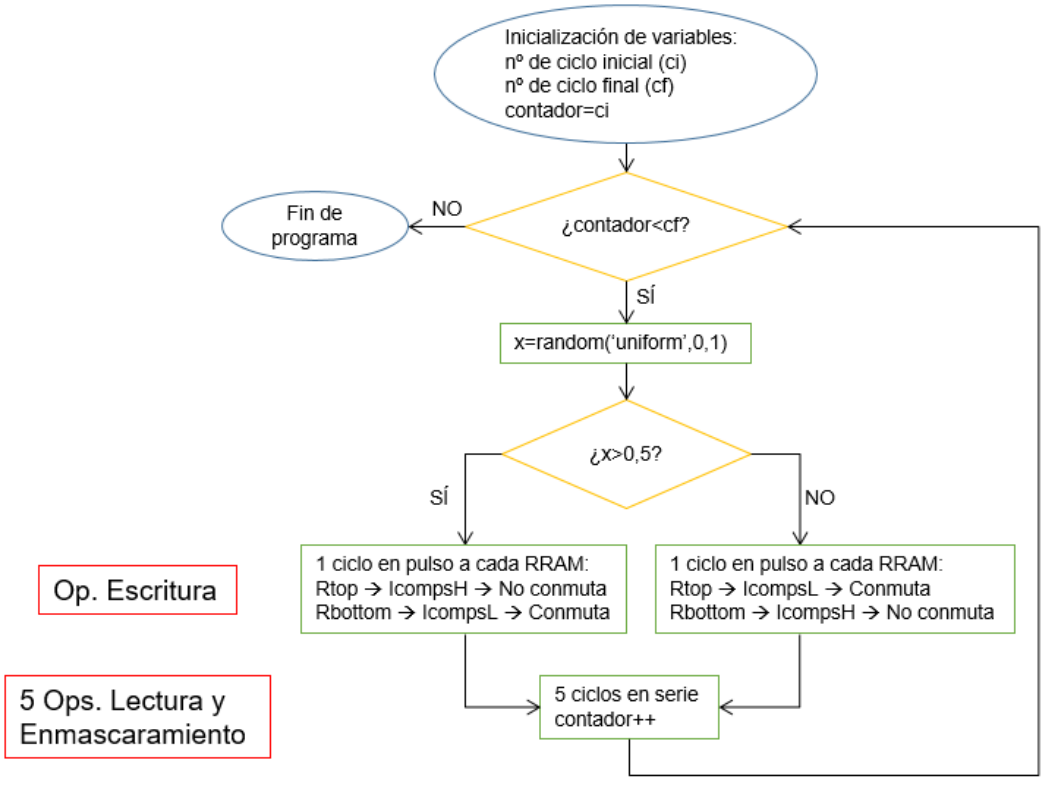


Figura 40. Diagrama de flujo del programa realizado en Matlab para realizar el experimento nº2

En la Figura 41, gráficas a) y b),Figura 41 se muestran los resultados para la operación de *reset* y de *set* de una pareja de RRAMs en serie al aplicar este experimento:

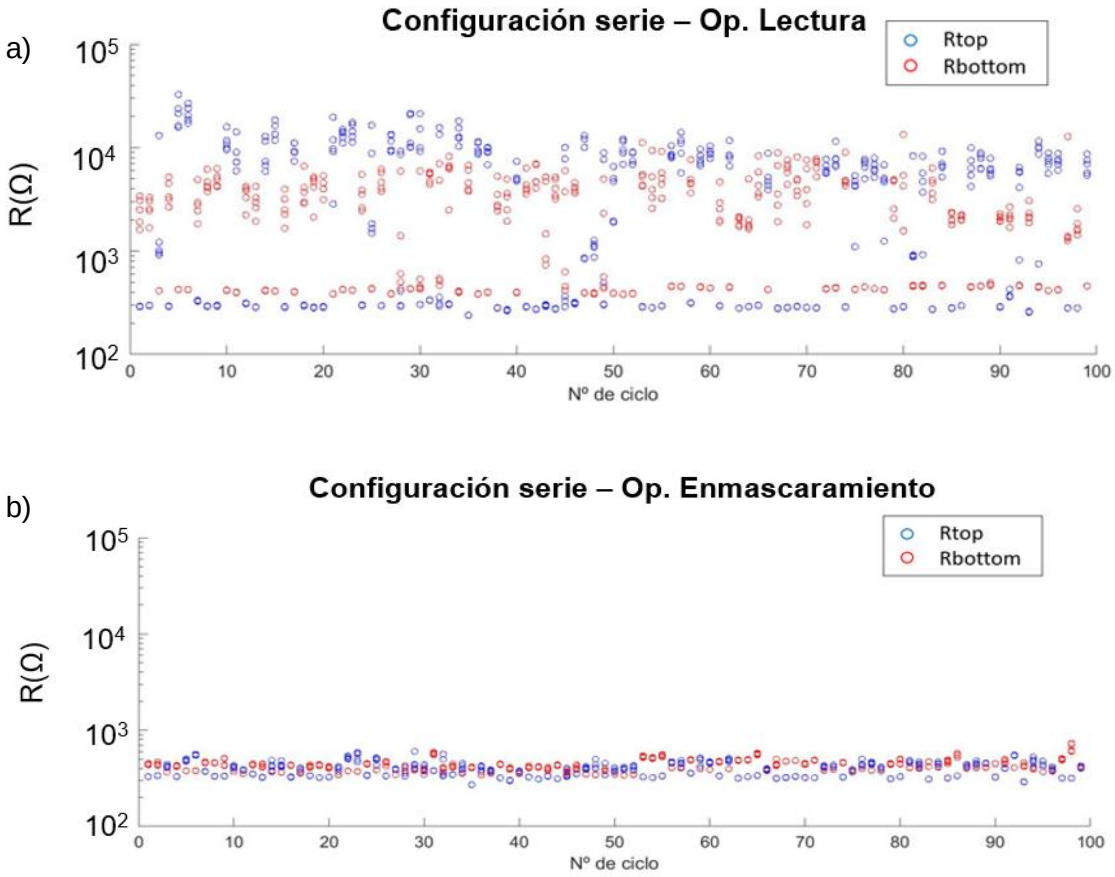


Figura 41. a) 100 ciclos en donde se puede ver la operación de lectura (reset) de las RRAMs en serie. b) 100 ciclos correspondientes a la operación de enmascaramiento (set) de las RRAMs en serie

En la Figura 41, gráfica a), se muestra la operación de lectura de la celda de memoria. En el eje X, se representan los ciclos de escritura que se han realizado de manera aislada a cada RRAM, que en el experimento son 100. En el eje Y se representa el valor resistivo de R_{top} (en azul) y el de R_{bottom} (en rojo). Por cada ciclo de escritura, se puede ver que hay 10 puntos: 5 puntos de color azul correspondientes a R_{top} y 5 puntos de color rojo correspondientes a R_{bottom}. Por ejemplo, en el ciclo de escritura 1, R_{top} tiene un valor resistivo bajo durante los cinco ciclos de lectura y R_{bottom} tiene un valor resistivo alto, y así durante los 100 ciclos de escritura y sus posteriores cinco ciclos de lectura. En la Figura 41, gráfica b), ocurre lo mismo pero con la operación de enmascaramiento. En el eje X se representan los ciclos de escritura y en el eje Y los valores resistivos de R_{top} y R_{bottom}. En este caso, se aprecia como cada vez que se realiza un enmascaramiento, R_{top} y R_{bottom} adquieren un estado resistivo bajo con un valor muy similar durante los cinco ciclos de enmascaramiento que se realizan tras la operación de lectura.

Como la visualización de los cinco ciclos de lectura y enmascaramiento, realizando un *reset* y *set* en serie, es complicada, se procesan los resultados obtenidos. Para ello, se realiza una gráfica (Figura 42) en el que se contabilizan las veces que ha conmutado la RRAM en la operación de lectura cuando ha sido limitada por la IcompsL en el ciclo de escritura. Es decir, si en el ciclo independiente de escritura se ha aplicado la IcompsL a R_{top}, ésta es la que debería conmutar durante los cinco ciclos siguientes de lectura. Y lo mismo sucede con la R_{bottom}. Por lo tanto, si de los cinco ciclos de lectura en serie, la RRAM conmuta en los cinco, quiere decir que es consistente y que la escritura del dato en la celda de memoria persiste.

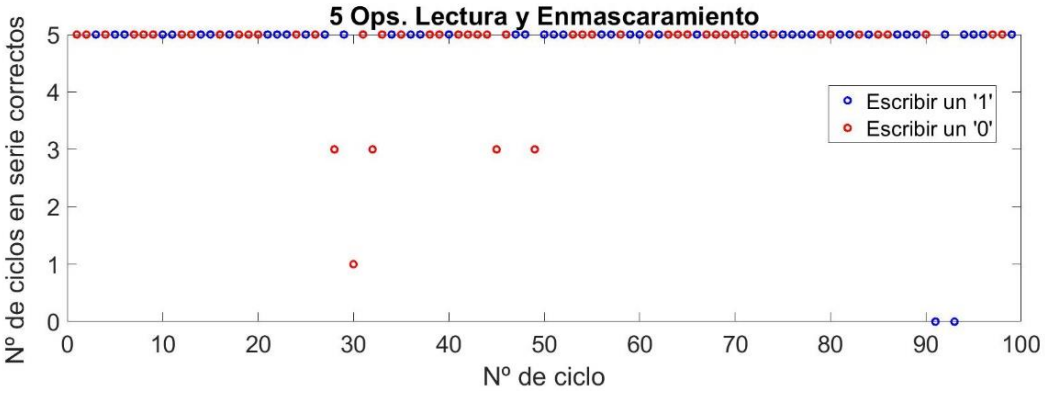


Figura 42. Contabilización del número de ciclos en serie que ha conmutado la RRAM que debería haberlo hecho por cada ciclo de escritura. Si la cifra es cinco, significa que ha conmutado siempre la RRAM que tenía que haberlo hecho, en otro caso significa que ha habido alguno de los ciclos de lectura que ha conmutado la otra RRAM

Se puede observar que prácticamente en todos los ciclos de escritura de la RRAM a la que se le ha aplicado la IcompsL, ha conmutado durante las cinco veces siguientes en serie. Cuando se ha escrito un '1' es R_{top} (color azul) la que debería conmutar las cinco veces, y cuando se ha escrito un '0' (color rojo) es R_{bottom} la que debería conmutar. De las 500 veces que se ha hecho conmutar a esta pareja de RRAMs en serie (100 ciclos de escritura independientes x 5 ciclos de lectura y enmascaramiento) ha habido 22 veces en las que la RRAM que debería haber conmutado no lo ha hecho. Esto representa un porcentaje de error de un 4,4% y se acepta como válido para confirmar la persistencia del dato en la celda de memoria propuesta.

Con estos resultados, se confirma el efecto que tiene la aplicación de la IcompsL en una de las RRAMs en ciclos consecutivos en serie, manteniendo su estado resistivo y probando la persistencia del dato en la celda de memoria.

7.3. Parámetros característicos de la celda de memoria

Se ha llevado a cabo un análisis de las tensiones y corrientes que se esperan para el circuito de control de la celda de memoria enmascarable.

Esta se basa en la disposición de dos RRAMs en serie, a las cuáles debe ser posible aislar entre sí de tal forma que se les pueda aplicar la IcompsH y la IcompsL a cada una de ellas en la operación de escritura por separado. Por lo tanto, aplicando a cada RRAM una Icomps diferente, se podrá controlar cuál de las dos conmutará al estado HRS y, consecuentemente, se podrá escribir un '1' o un '0' cuando se quiera. Sin embargo, un atacante no podrá conocer cuál de las dos conmutará de forma fiable, ya que se ha observado que con las corrientes de IcompsL (250µA) e IcompsH (1mA) utilizadas, se consiguen valores resistivos de las RRAMs en el estado LRS suficientemente parecidos como para dificultar la lectura de la información guardada.

Los niveles de tensión que requiere el circuito de control son los que se han utilizado para realizar las experimentaciones con las RRAMs. Por lo tanto, se necesitará una tensión para la operación de *set* de 1,1V y una tensión para la operación de *reset* de -1,4V. Sin embargo, empíricamente se conoce que las tensiones umbrales V_{SET} y V_{RESET} son menores que estas tensiones para la operación de escritura de las RRAMs, por lo que será posible utilizar una tecnología con una tensión de alimentación menor.

Una vez analizados los valores resistivos experimentales de las RRAMs para los estados HRS y LRS, y teniendo en cuenta que en el estado LRS va a haber dos niveles, uno para cada valor de Icomps, las resistencias previstas son:

- Resistencia en el estado HRS: 10000Ω
- Resistencia en el estado LRS: cuando la RRAM se ve afectada por la IcompsL, la resistencia es de 500Ω. Si se ve afectada por la IcompsH, la resistencia es de 200Ω.

Estos valores son una media de las medidas realizadas, aunque se ha observado una alta variabilidad *device-to-device* y *cycle-to-cycle*.

8. Celda de memoria enmascarable de un bit

8.1. Propuesta de circuito de control y dimensionamiento de los transistores

Conociendo los valores típicos de resistencia de las RRAMs tanto en el estado LRS como en el estado HRS, es posible calcular la corriente que circula a través de los transistores conociendo la tensión de alimentación de la tecnología utilizada. En este proyecto, se han utilizado transistores de la tecnología CMOS de 65nm con una tensión de alimentación de 1,2V y se han realizado las simulaciones del circuito con el software *"Cadence Virtuoso Analog Design Environment"*. El circuito de control propuesto es el siguiente, en dónde R1 representará a R_{top} y R2 representará a R_{bottom}:

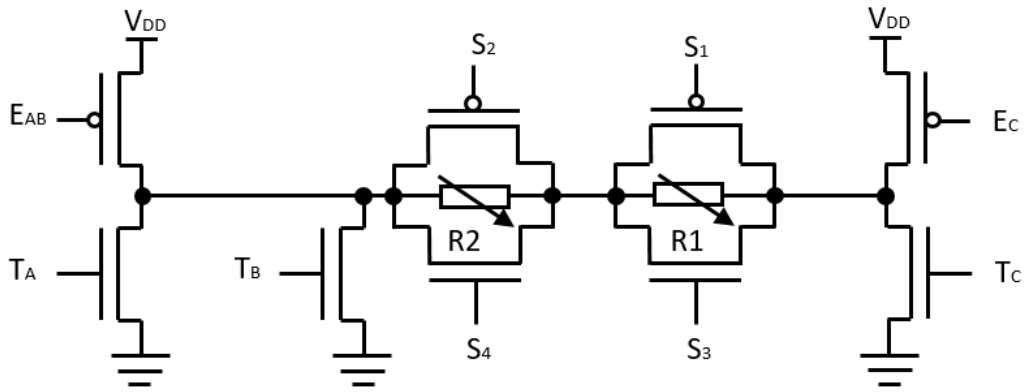


Figura 43. Circuito de control propuesto para el enmascaramiento, lectura y escritura de las dos RRAMs

Se compone de transistores NMOS y PMOS, a los cuáles se les ha nombrado igual que las señales que reciben (El transistor E_{AB} recibe una señal E_{AB}, y así con todos). Con el fin de poder intervenir en cada una de las RRAMs por separado para realizar las operaciones de escritura, se propone que tanto R1 como R2 tengan en paralelo una puerta de transmisión formada por dos transistores NMOS y PMOS. De esta forma, la puerta de transmisión actuará a modo de *"bypass"* cuando haya que actuar sobre una de las dos RRAMs en las diferentes operaciones de *set* y *reset* independientes. Para limitar la corriente que circula por una de las dos RRAMs, se utilizan los transistores T_A y T_B. Si estos están en funcionamiento, la corriente que circula en la operación de escritura en el *set* es IcompsH, mientras que, si sólo está en funcionamiento T_A, la corriente que circula en la operación de escritura en el *set* por la RRAM es IcompsL. Los niveles de tensión para el '1' y '0' lógicos son 1,2V y 0V respectivamente. Por lo tanto, el funcionamiento lógico de las señales de cada transistor del circuito para las diferentes operaciones de la celda de memoria es el indicado en la Tabla 4:

:

Lógica binaria de los transistores del circuito			E_{AB}	E_C	T_A	T_B	T_C	S_1	S_2	S_3	S_4
RRAMs independientes	***RESET*** (Op. Escritura)	R1	0	1	0	0	1	1	0	0	1
		R2	0	1	0	0	1	0	1	1	0
	SET (Op. Escritura)	R1	1	0	1	**0/1**	0	1	0	0	1
		R2	1	0	1	**1/0**	0	0	1	1	0
RRAMs en serie	***RESET*** *(Op. Lectura)*		0	1	0	0	1	1	1	0	0
	SET *(Op. Enmascaramiento)*		1	0	1	1	0	1	1	0	0

Tabla 4. Lógica de las señales que tienen que recibir los transistores para realizar las operaciones de escritura, lectura y enmascaramiento

Primero se ha dimensionado el transistor PMOS E_C y, a partir de este, el PMOS E_{AB} y los NMOS T_A, T_B y T_C. Para el dimensionamiento de E_C, se ha de tener en cuenta los valores resistivos de la RRAM en el estado LRS y HRS, con tal de estimar la corriente máxima y mínima que puede circular si no se limita la corriente. Se obtienen los siguientes valores de corriente para los dos estados:

$$I_D(\max) = \frac{V_{DD}}{R_{LRS}(\mathrm{IcompsH})} = \frac{1{,}2V}{200\Omega} = 6mA \qquad \text{(Ec.3)}$$

$$I_D(\min) = \frac{V_{DD}}{R_{HRS}} = \frac{1{,}2V}{10k\Omega} = 0{,}12mA \qquad \text{(Ec.4)}$$

A partir de estas dos corrientes, se puede hallar la recta de carga del transistor. Se necesita que pueda soportar al menos la IcompsH que se establece en 1mA. Se realiza primero una simulación de un transistor PMOS en *Cadence*. En la Figura 44 se muestra el esquemático del circuito simulado:

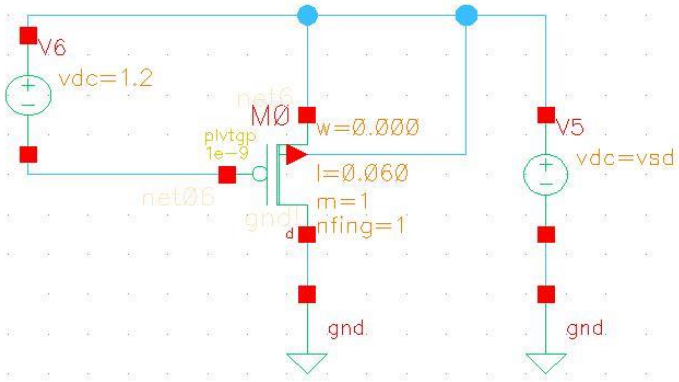


Figura 44. Esquemático de la simulación del transistor PMOS E_C

Se establece una tensión fuente-puerta (V_{sg}) de 1,2V y se parametriza el ancho del canal (w) del transistor PMOS para observar las curvas características en función de este parámetro. La parametrización lineal abarca los anchos de canal, desde el mínimo para esta tecnología que es 0,130µm hasta 12,61µm con pasos de 0,520µm (aumentando el ancho mínimo del canal por 5 en cada paso de parametrización). En la Figura 45 se observan las curvas características del transistor para los diferentes anchos de canal:

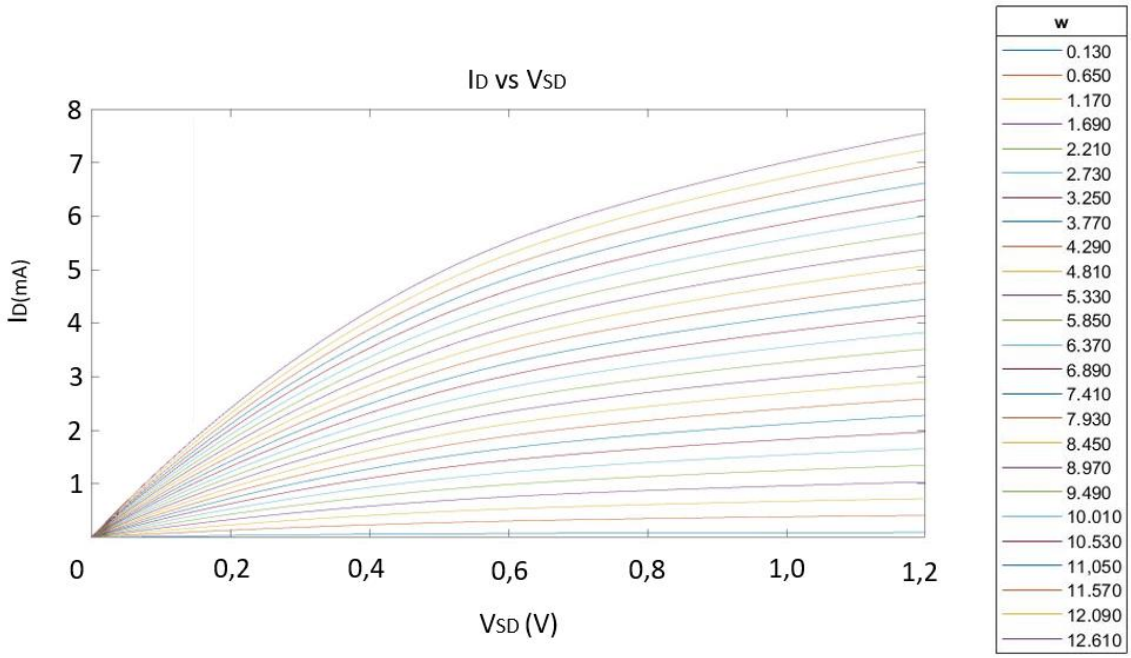


Figura 45. Curvas características del transistor PMOS. Cada una de ellas representa un ancho de canal diferente, siendo el canal más pequeño el que menor corriente conduce, y el canal más grande el que mayor corriente conduce (w(µm))

Para establecer los límites en los que trabaja el transistor E_C, se debe acotar su región de operación. En teoría, la corriente máxima de drenador (I_D(máx)) tiene un valor de 6mA y la corriente mínima de drenador (I_D(min)) un valor de 0,12mA. Sin embargo, sólo es necesario que circule como máximo 1mA por el transistor cuando la RRAM se limite con IcompsH en el

estado LRS. Para estar seguros de que conduzca esta corriente, se considera un sobredimensionamiento del transistor de un 50%, por lo que la corriente que pueda circular sea 1,5mA. En la Figura 46, se muestran las curvas características del transistor para los diferentes anchos de canal, así como las rectas de carga, la IcompsH y su sobredimensionamiento. En negro se ha marcado el triángulo de operación del transistor, por lo que se puede escoger entre unos cuantos anchos de canal para proseguir con el diseño del circuito de control.

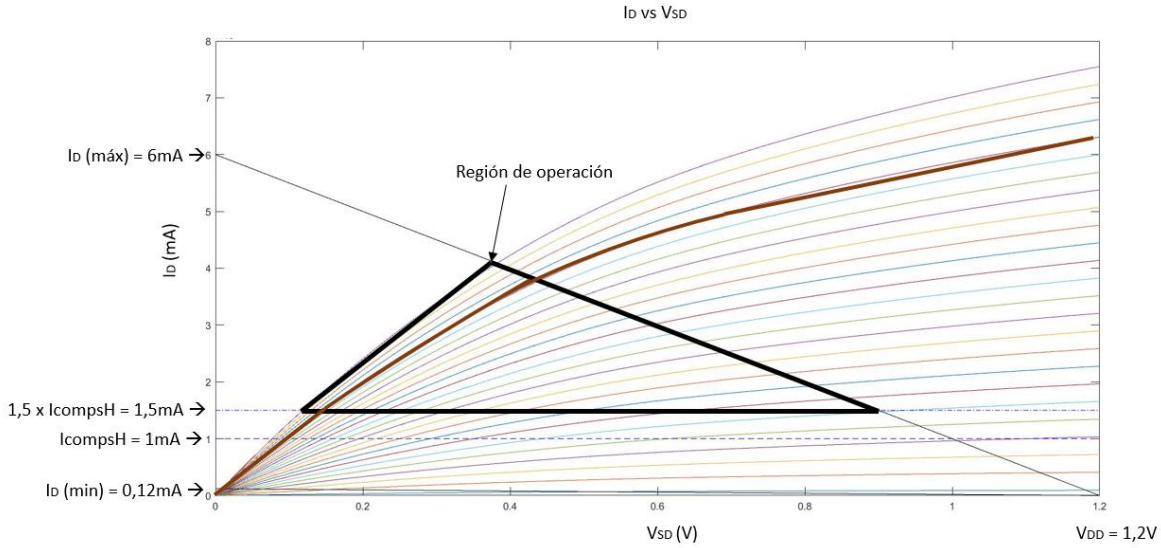


Figura 46. Curvas características del transistor PMOS para los diferentes anchos de canal. Se ha marcado el triángulo para observar los posibles anchos de operación que interesan para dimensionar este transistor

Como interesa que el transistor PMOS trabaje en la zona óhmica, se selecciona el de color marrón con un ancho de canal de 10,530µm y se representa en la Figura 47 los puntos de trabajo sobre la curva característica:

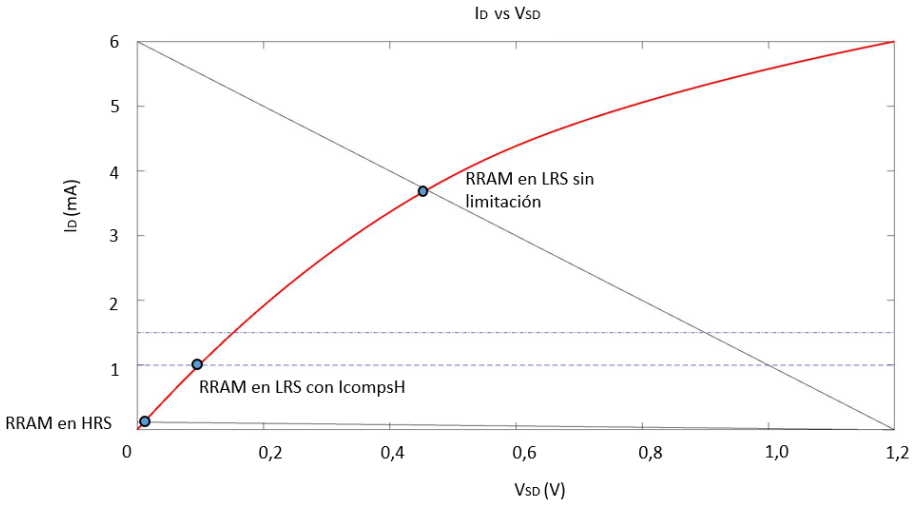


Figura 47. Curva característica del transistor PMOS seleccionado con un ancho de canal w=10,530 µm. Se han marcado los puntos en los que trabajará el transistor en LRS y HRS

A continuación, se procede al dimensionamiento del transistor NMOS T_A. Para ello se realiza un análisis paramétrico que tiene por objetivo determinar el ancho de canal del transistor NMOS para que circule la corriente que se desea, en este caso IcompsL.

Se simula un circuito utilizando el PMOS dimensionado previamente y un NMOS con un ancho de canal (w) variable. Por lo tanto, mediante un análisis en barrido DC, en la Figura 49 se representa, en el eje Y, la intensidad que circula por el NMOS y, en el eje X, los diferentes anchos de canal desde el mínimo (w=0,130µm) hasta un ancho de 2µm. Como T_A es el transistor que limita la corriente a IcompsL, su ancho deberá ser menor que el de T_B. En concreto, si la relación de corrientes entre la IcompsH y la IcompsL es cuatro, el transistor T_B deberá conducir tres veces más corriente que el T_A, de modo que cuando ambos estén en funcionamiento la corriente que circule por la RRAM sea IcompsH. Se utiliza una resistencia con un valor de 500Ω para simular el nivel de resistencia alto de la RRAM en el estado LRS, por lo que la corriente que pasará por el transistor será IcompsL (250µA). En la Figura 48 se muestra el esquema de la simulación y en la Figura 49 la representación de la corriente que circula por el transistor NMOS en función del ancho de canal del transistor:

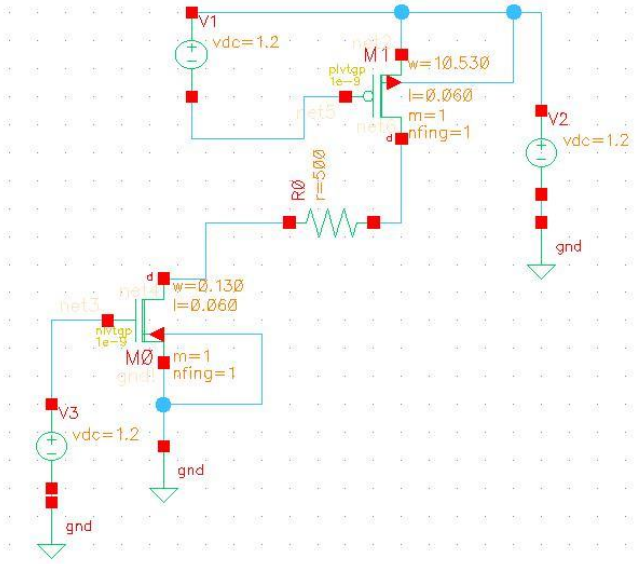


Figura 48. Esquema del circuito de simulación utilizando el PMOS dimensionado anteriormente y en función del cual se dimensiona el transistor T_A

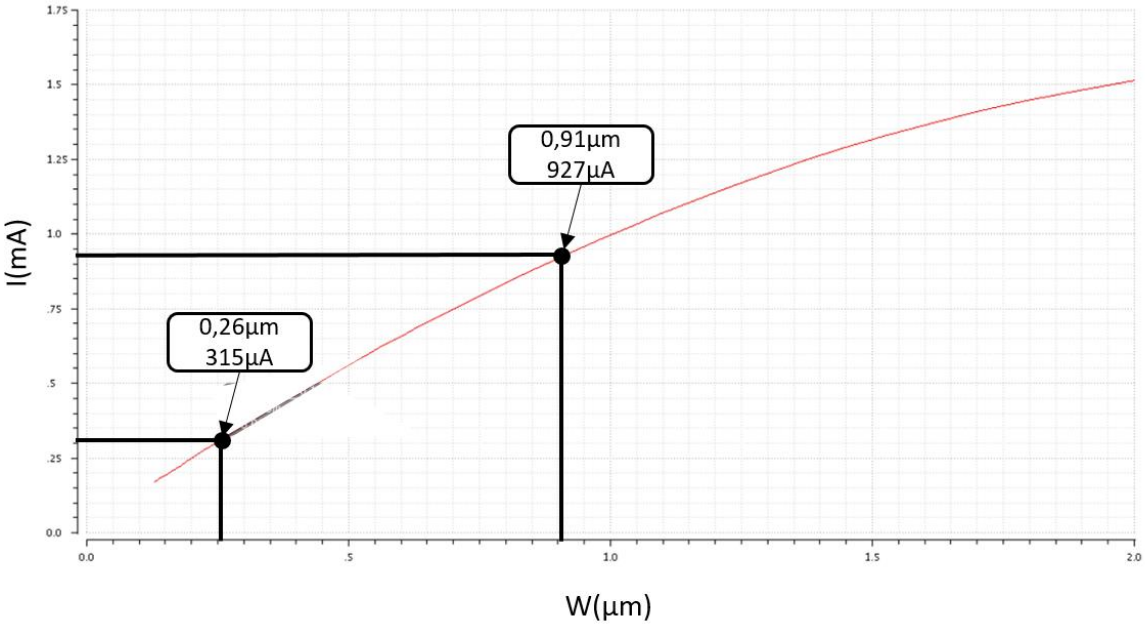


Figura 49. Representación de la corriente que circula por el transistor en función del ancho de canal

El ancho de canal (w) para que conduzca 250µA es de 0,201µm lo que supone un transistor 1,5 veces más grande que el de canal mínimo. Como los transistores se fabrican con anchos de canal múltiplos del mínimo, se escoge un transistor con un ancho de canal de 0,260µm. Con este ancho de canal, la IcompsL obtendrá un valor de 315 µA. El transistor T_B se dimensiona para que sea capaz de conducir una corriente tres veces mayor que el T_A de forma que con ambos dos se sume el valor de IcompsH. La corriente que debe circular por la RRAM para que se cumpla la relación entre la IcompsL y la IcompsH de cuatro, debe ser de 1260µA (4 x 315µA). En la simulación se observa que el ancho de canal debe que tener T_B para que conduzca 945µA (3 x 315 µA) es de 0,933µm, pero como debe ser múltiplo del ancho de canal mínimo, se selecciona el de 0,910µm que tiene una capacidad de corriente de 927µA. Por lo tanto, la relación real que se obtendrá será:

- $IcompsL\ (T_A) = 315\mu A$
- $IcomspH\ (T_A + T_B) = 315\mu A + 927\mu A = 1242\mu A$
- $IcompsH / IcompsL = 3{,}94$

La corriente que circula por la RRAM aislada cuando se encuentra en el estado HRS es muy baja, y en este caso tan solo entran en juego los transistores E_{AB} y T_C. El transistor E_{AB} es un PMOS dimensionado igual que el transistor E_C ya que ambos soportan los mismos niveles de corriente en el estado LRS (que es cuando mayor corriente circula). El transistor T_C es un NMOS que se dimensionará 200 veces mayor que el transistor T_B, teniendo un ancho de canal de 26µm ya que no debe limitar la corriente y, realizando diferentes simulaciones, se observa que este valor es el óptimo para realizar operaciones de *reset* tanto de forma independiente

a cada RRAM como en serie. Los transistores PMOS, S_1 y S_2, se dimensionan con un ancho de canal de 63,18µm y los NMOS, S_3 y S_4, con un ancho de canal de 26µm. Estos cuatro transistores se dimensionan de forma iterativa. Se fue incrementando el ancho de canal tanto de los transistores PMOS como de los NMOS para que actuasen de forma correcta como *bypass*. Al final, se optó por dimensionar a S_1 y S_2 con el mismo tamaño que el resto de PMOS del circuito (E_C y E_{AB}) y a S_3 y S_4 como el NMOS T_C. Estos valores pueden variar en función de los niveles de corriente que se impongan en el circuito y del valor resistivo de las RRAMs.

Estos anchos de canal tan grandes se deben a que la tecnología actual utilizada para la fabricación de RRAMs no está madura, y los valores resistivos no tienen la magnitud que se desearía. Cuanto más grande sean estos valores tanto para el estado HRS como para el LRS, menor será la corriente que circulará por el circuito de control de la celda de memoria y, por lo tanto, menor será el área ocupada por los transistores empleados.

8.2. Simulación de la celda de memoria

En la Figura 50 se muestra el circuito diseñado con los transistores dimensionados y las RRAMs en el entorno de simulación *Cadence*:

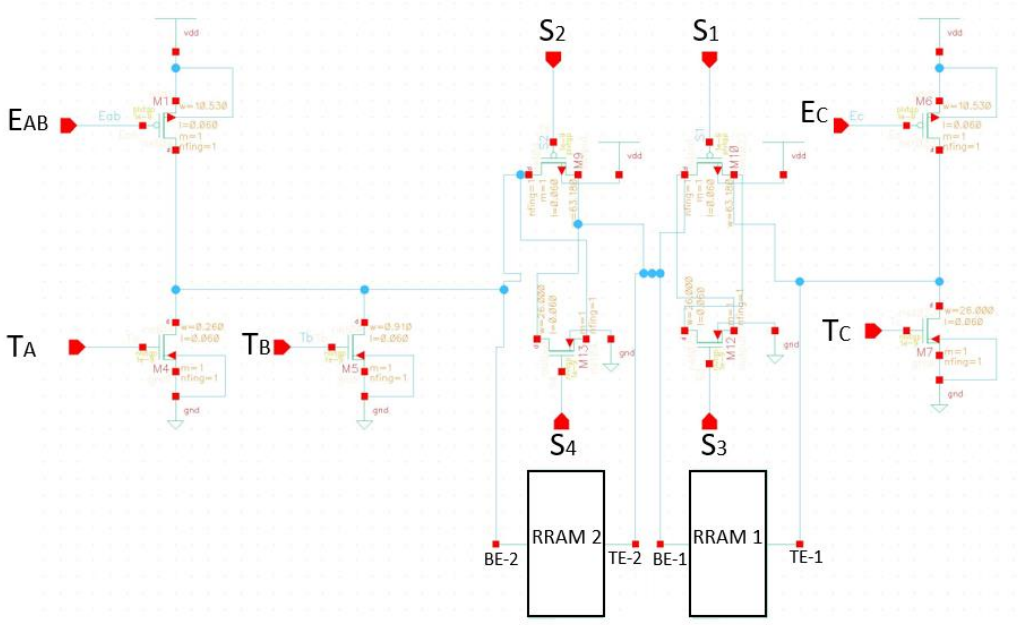


Figura 50. Esquemático del circuito de control propuesto para la lectura, escritura y enmascaramiento de las RRAMs en el entorno de simulación Cadence

Antes de realizar la simulación del circuito de control y comprobar que las operaciones de escritura, lectura y enmascaramiento funcionan correctamente, se realiza la simulación eléctrica del modelo en VerilogA de la RRAM proporcionado por la Universidad de Granada [23]. De este modelo, se han cambiado determinados parámetros para que su

comportamiento en simulación se asemeje los más posible a las RRAMs con las que se ha experimentado. Se ha cambiado la longitud del *gap* y el radio del CF, para actuar sobre los valores resistivos que la RRAM presenta en los estados LRS y HRS. Los parámetros finales del modelo son los siguientes:

- $gap_{min} = 2{,}5\ x\ 10^{-10}\ m$
- $gap_{max} = 3\ x\ 10^{-9}\ m$
- $RCF_{min} = 4{,}5\ x\ 10^{-9}\ m$
- $RCF_{max} = 5{,}5\ x\ 10^{-9}\ m$

En la Figura 51 se puede observar la curva característica de la RRAM:

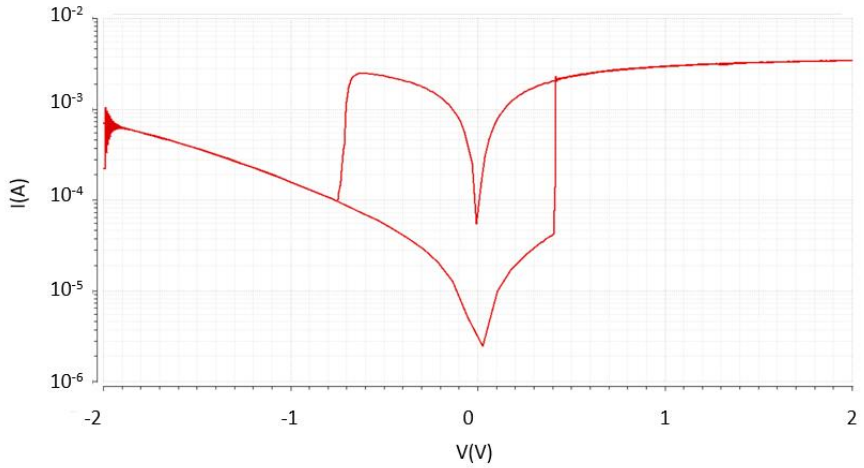


Figura 51. Curva característica I-V de las RRAMs utilizadas en la simulación

Por lo tanto, las características que definen a esta RRAM en simulación son los siguientes:

- Resistencia en el estado HRS ≈ 10kΩ
- Resistencia en el estado LRS ≈ 200Ω
- V_{RESET} ≈ -700 mV
- V_{SET} ≈ 400 mV

En la simulación del circuito de control propuesto para controlar la celda de memoria, se ha realizado el siguiente proceso para escribir un '1' o un '0', leerlo y enmascarar el dato:

- Simulación nº1 (Figura 52): Se ha escrito un '1' en la celda memoria. Para ello, se ha realizado en primer lugar una operación de escritura formada por un *reset* y un *set* independientes, en donde se ha aplicado la IcompsL en la R1 y la IcompsH en la R2. Después se realiza la operación de lectura aplicando una tensión de *reset* en serie y, por último, se vuelve a enmascarar la celda de memoria aplicando una tensión de *set* en serie para dejar las dos RRAMs en el estado LRS.

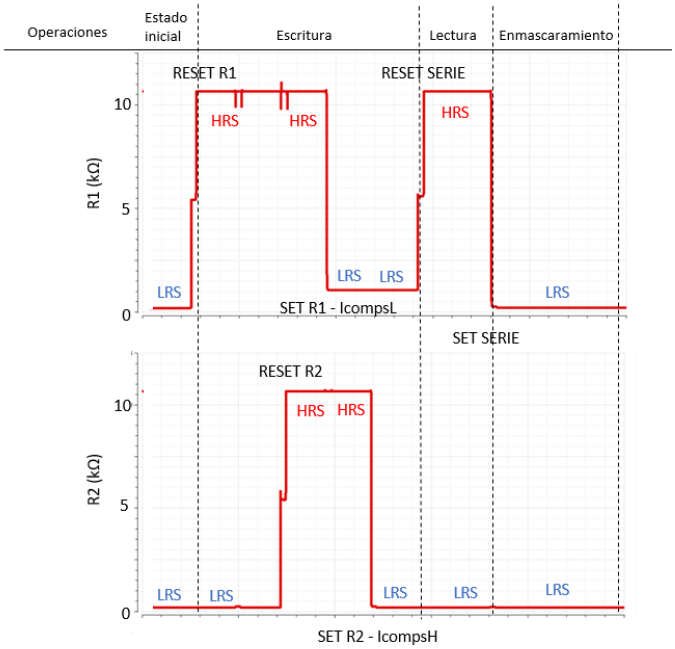


Figura 52. Forma de onda de la simulación de la escritura, lectura y enmascaramiento de un '1'

Se observa que al hacer un *set* de R1 y un *set* de R2 de manera independiente, el valor resistivo de R1 es mayor (1kΩ de R1 frente a 200Ω de R2) ya que se ha aplicado la IcompsL y, por lo tanto, en la operación de lectura de la celda es la que conmuta. A continuación, al realizar una operación de enmascaramiento, realizando un *set* en serie, las dos RRAMs vuelven al estado LRS con una resistencia muy semejante. Por lo tanto, la escritura de un '1', la lectura, y el posterior enmascaramiento son correctos.

- **Simulación nº2** (Figura 53): Se ha escrito un '0' en la celda memoria. Para ello, se ha realizado en primer lugar una operación de escritura formada por un *reset* y un *set* independientes, aplicando la IcompsL en la R2 y la IcompsH en la R1. A continuación, se realiza la operación de lectura aplicando una tensión de *reset* en serie y, por último, se vuelve a enmascarar la celda de memoria aplicando una tensión de *set* en serie para volver las dos RRAMs al estado LRS.

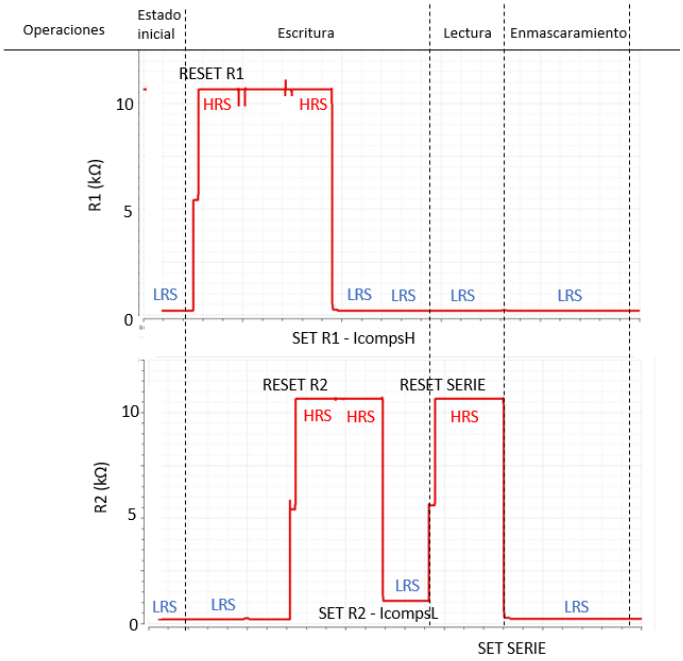


Figura 53. Forma de onda de la simulación de la escritura, lectura y enmascaramiento de un '0'

De forma semejante a la escritura de un '1', al escribir un '0' en la celda de memoria se observa que el valor resistivo de R2 es mayor (1kΩ de R1 frente a 200Ω de R2) después de realizar un *set* independiente a las RRAMs, y por lo tanto en la lectura de la celda, al realizar un *reset* en serie, es la que conmuta. Por ello, la escritura de un '0', la lectura, y el posterior enmascaramiento son correctos.

Se aprecia que en la Figura 52 y en la Figura 53, la celda de memoria sigue el comportamiento esperado para almacenar un '1' o un '0', y por lo tanto el circuito realizado es válido para controlar las RRAMs en serie como celda de memoria enmascarable. A pesar de que los valores resistivos en LRS son un poco mayores a los esperados, esto se debe a que los transistores que forman el circuito no son ideales y además se han sobredimensionado, de forma que es lógico que las resistencias varíen. Por lo tanto, se considera que el dimensionamiento de los transistores para estos valores resistivos de las RRAMs es correcto, y, como se puede observar mediante las simulaciones eléctricas del circuito, el comportamiento es el esperado.

9. Estudio económico

El estudio económico del proyecto realizado en el grupo de investigación QinE, tiene en consideración los costes asociados a la instrumentación utilizada en el laboratorio, así como los programas de software y todos los componentes empleados. Incluye también los recursos humanos requeridos en el proyecto.

9.1. Costes asociados a la instrumentación, licencias del software y componentes del laboratorio

La instrumentación utilizada en el laboratorio durante el proyecto ha sido la siguiente:

- Dos SMUs.
- Ordenador para controlar las SMUs.
- Estación de puntas.
- Posicionadores de las puntas.
- Armario metálico.
- Mesa antivibratoria.
- Bomba de vacío.
- Compresor.

A pesar de que estos instrumentos se han utilizado durante los meses de duración del proyecto, se ha hecho el cómputo únicamente la parte proporcional asociada a este tiempo de uso. Además, debido a que la estación de puntas se utiliza desde hace más de 15 años, se considera que está totalmente amortizada y no supone un coste para el cómputo global.

Respecto al software utilizado, se ha hecho uso de la licencia académica de *MatLab* en su versión R2018b y la licencia de uso profesional de *Cadence Virtuoso*.

Los componentes utilizados durante el proyecto han sido los siguientes:

- Oblea en donde se encuentran las RRAMs utilizadas para la realización de las pruebas experimentales. Se ha utilizado la mitad de una oblea entera, y de esta mitad se considera que se ha hecho uso del 10% de las RRAMs que hay. Por lo tanto, si en media oblea hay aproximadamente 4100 RRAMs, se han utilizado 410 RRAMs durante el proyecto.
- Cables y adaptador GPIB-USB que permiten la interconexión de los diferentes instrumentos.

En la Tabla 5 se encuentra el desglose del coste asociado a estos conceptos:

Coste de la instrumentación, licencias de software y componentes					
Concepto	**Coste unitario (€)**	**Unidades empleadas**	**Periodo de uso (meses)**	**Periodo de depreciación (meses)**	**Importe (€)**
SMU	12000	2	3,5	120	700
Ordenador	2000	1	5	60	166,67
Estación de puntas	10000	1	3,5	Amortizada	0
Armario metálico	1636	1	3,5	180	31,81
Posicionadores de las puntas	1000	4	3,5	120	116,67
Mesa antivibratoria	4700	1	3,5	120	137,08
Bomba de vacío	650	1	3,5	60	37,92
Compresor	200	1	3,5	60	11,67
Licencia de MatLab	500	1	3,5	12	145,83
Licencia de Cadence	600	1	2	12	100
RRAMs utilizadas	0,25	410	N/A	N/A	102,5
Cables y adaptador GPIB-USB	693,33	1	3,5	60	40,44
Subtotal (€)					**1590,59**

Tabla 5. Costes asociados a la instrumentación, software y componentes utilizados

9.2. Costes asociados a los recursos humanos

Respecto a los costes asociados a los Recursos Humanos en este trabajo, se ha contabilizado tanto los costes del estudiante como de los tutores implicados, en aspectos de orientación y asesoría de los profesores al estudiante. Se ha realizado el estudio separando las labores que han sido realizadas por el estudiante y por el profesorado, considerando que un ingeniero junior cobra 25€/h, y un ingeniero senior cobra 60€/h. En total, se han realizado 900 horas repartidas entre los 5 meses de duración del proyecto. En la Tabla 6 se encuentra el desglose del coste asociado a los recursos humanos:

Costes asociados a los recursos humanos			
Concepto	**Horas**	**Importe Ingeniero Junior – 25€/h (€)**	**Importe Ingeniero Senior – 60€/h (€)**
Estudio del estado del arte	80	2.000	-
Formación en el instrumental y equipos de medida	10	250	-
Experimentaciones con RRAMs aisladas	200	5.000	-
Experimentación con RRAMs en serie	200	5.000	-
Diseño de la celda de memoria enmascarable	150	3.750	-
Documentación de resultados	40	1.000	-
Redacción de la memoria	120	3.000	-
Tutorías del profesorado al estudiante	50	-	3.000
Dirección del proyecto (2 directores)	50	-	3.000
Subtotal parcial (€)		20.000	6.000
Subtotal (€)		**26.000**	

Tabla 6. Costes asociados a los recursos humanos requeridos en el proyecto

9.3. Coste total del proyecto

Se contabilizan de forma aproximada los costes indirectos que se imputan al proyecto que ha tenido lugar en el Departamento de Electrónica de la UPC. Se aplica un 17,7% a la suma de los costes de instrumentación, licencias del software y componentes, y al coste de los recursos humanos. En la Tabla 7 se recogen todos los costes asociados al proyecto:

Coste total del proyecto	
Concepto	**Importe (€)**
Costes de instrumentación, licencias del software y componentes	1.590,59
Costes de recursos humanos	26.000
Costes indirectos (17,7%)	4.883,53
Total (€)	**32.474,12**

Tabla 7. Coste total del proyecto

Conclusiones

Como conclusión final del trabajo, se puede afirmar que la celda de memoria no volátil enmascarable de un bit utilizando RRAMs en serie es viable. Sin embargo, primero se han realizado una serie de experimentaciones con los dispositivos tanto de manera independiente como en serie que permiten realizar esta afirmación.

En primer lugar, se ha observado experimentalmente que con los dispositivos aislados y actuando independientemente sobre cada uno de ellos, se puede modular la resistencia en el estado LRS de las RRAMs, de forma que aumente cuando aplicamos un valor bajo de corriente de *compliance* en la operación de *set* (IcompsL).

En segundo lugar, en la configuración en serie de dos RRAMs no conmuta cualquiera de las dos, sino aquella con un valor de resistencia mayor en el estado LRS. Esto se ha demostrado que es independiente de la posición de la RRAM (R_{top} o R_{bottom}) en la configuración serie, y que lo hace de forma sistemática durante todos los ciclos de experimentación.

En tercer lugar, se ha demostrado experimentalmente que podemos forzar la conmutación de la RRAM deseada, pudiendo así guardar un ‘0’ o un ‘1’ cuando deseemos. También se ha demostrado experimentalmente la persistencia del dato guardado durante cinco ciclos de lectura y enmascaramiento consecutivos tras una operación de escritura. Por lo tanto, son dispositivos fiables para almacenar información en memorias no volátiles.

Por último, se ha realizado una propuesta del circuito de control para la celda de memoria que permite realizar las operaciones de escritura, lectura y enmascaramiento de acuerdo a lo previamente especificado. Se ha validado su correcto funcionamiento mediante simulación en las escrituras de un ‘1’ o un ‘0’.

Por lo tanto, modulando la resistencia en el estado LRS mediante la Icomps se puede escribir un ‘1’ o un ‘0’ en la celda de memoria y posteriormente realizando una operación de enmascaramiento, el bit de información queda protegido ante un posible ataque mediante ingeniería inversa.

En conclusión, las RRAMs son dispositivos emergentes en el mundo de las memorias no volátiles y su uso en un futuro cercano se prevé muy amplio. Como trabajo futuro se plantea el rediseño de los circuitos de control para RRAMs con un valor resistivo mayor que facilite la reducción del área de los transistores. También comentar que en este trabajo no se ha experimentado con la estabilidad en el tiempo, con la temperatura o la robustez frente a otros tipos de ataques, tareas que se deberán considerar en la siguiente fase de desarrollo de este tipo de celda.

Agradecimientos

Me gustaría agradecer por la oportunidad de trabajar en el grupo de investigación QinE y realizar este Trabajo de Fin de Máster a mis directores del proyecto, Daniel Arumí Delgado y Salvador Manich Bou. Además, quisiera también agradecerles por todas las recomendaciones, consejos, lecciones y seguimiento que han realizado a lo largo de todo el proceso. Todos los artículos, documentación, instrumentación para llevar a cabo los experimentos y, sobre todo, por el tiempo que han dedicado a resolver mis dudas y analizar los resultados de las pruebas realizadas.

También, me gustaría agradecer por la ayuda que me ha ofrecido Álvaro Gómez-Pau para afianzar los conceptos aprendidos durante el grado y el máster, así como en la ayuda prestada en los programas de Matlab y Cadence Virtuoso.

Por último, también agradezco los conocimientos que ha puesto a mi disposición Rosa Rodríguez Montañés para entender el funcionamiento de las RRAMs.

Bibliografía

[1] D. Arumí, M.B. Gonzalez, F. Campabadal, “RRAM serial configuration for the generation of random bits”, in *Microelectronic Engineering*, vol. 178, pp. 76-79, 2017

[2] D. Arumí, Á. Gómez-Pau, S. Manich, R. Rodríguez-Montañés, M. B. González and F. Campabadal, "Unpredictable Bits Generation Based on RRAM Parallel Configuration," in *IEEE Electron Device Letters*, vol. 40, no. 2, pp. 341-344, Feb. 2019

[3] S. Galeano. Marketing for e-commerce, URL: https://marketing4ecommerce.net/usuarios-internet-mundo/, Consulta: 13-05-2019

[4] E. Tena, (2019), Diseño y caracterización de criptocircuitos seguros y resistentes a ataques físicos (Tesis doctoral) Universidad de Sevilla, Instituto de Microelectrónica de Sevilla

[5] J.P.Morgan,(2018).Payments fraud and control survey report, URL: https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/afp-survey-2018.pdf, Consulta: 10-04-2019

[6] S.P. Skorobogatov, “Semi-invasive attacks – A new approach to hardware security analysis”, in *Universidad de Cambridge*, no. 630, Apr. 2005

[7] U. Rührmair and M. van Dijk, "PUFs in Security Protocols: Attack Models and Security Evaluations," *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2013, pp. 286-300

[8] C. Helfmeier, C. Boit, D. Nedospasov, S. Tajik and J. Seifert, "Physical vulnerabilities of Physically Unclonable Functions," *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Dresden, 2014, pp. 1-4.

[9] *L. Chua, "*Memristor-The missing circuit element*,"* en *IEEE Transactions on Circuit Theory,* vol. 18, no. 5, pp. 507-519, Sep. 1971.

[10] Strukov, Dmitri B., Snider, Gregory S., Stewart, Duncan R., Williams, R. Stanley, *“*The missing memristor found*”* in *Nature Publishing Group,* vol.453, - 008/05/01/online

[11] S. Yu, "Overview of resistive switching memory (RRAM) switching mechanism and device modeling," *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, Melbourne VIC, 2014, pp. 2017-2020.

[12] *Gale, Ella. (2011). The missing magnetic flux in the HP memristor found.*

[13] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy and D. Ielmini, "Statistical Fluctuations in HfOx Resistive-Switching Memory: Part I - Set/Reset Variability" in *IEEE Transactions on Electron Devices*, vol. 61, no. 8, pp. 2912-2919, Aug. 2014.

[14] S. Balatti *et al*., "Understanding pulsed-cycling variability and endurance in HfOx RRAM," *2015 IEEE International Reliability Physics Symposium*, Monterey, CA, 2015, pp. 5B.3.1-5B.3.6.

[15] S.T. Hsu, W. Pan, F. Zhang, W. Zhuang y T. Li, “RRAM memory cell electrodes”, US 6 849 891, Feb. 2005

[16] S. Kvatinsky, G. Satat, N. Wald, E. G. Friedman, A. Kolodny and U. C. Weiser, "Memristor-Based Material Implication (IMPLY) Logic: Design Principles and Methodologies," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 10, pp. 2054-2066, Oct. 2014.

[17] L. Xie, H. A. D. Nguyen, J. Yu, M. Taouil and S. Hamdioui, "On the robustness of memristor based logic gates," *2017 IEEE 20th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*, Dresden, 2017, pp. 158-163.

[18] C. Li et al*., “*Efficient and self-adaptive in-situ learning in multilayer memristor neural networks”*, Nature Communications,* vol. 9, no.1, Jun. 2018

[19] H. Abunahla y B. Mohammad*,* “Memristor Technology: Synthesis and Modeling for Sensing and Security Applications*”, Ed. Springer,* NY, USA: 2018 p.77

[20] A. Chen, "Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions," in *IEEE Electron Device Letters*, vol. 36, no. 2, pp. 138-140, Feb. 2015.

[21] A. Bricalli, E. Ambrosi, M. Laudato, M. Maestro, R. Rodriguez and D. Ielmini, "Resistive Switching Device Technology Based on Silicon Oxide for Improved ON–OFF Ratio—Part I: Memory Devices," in *IEEE Transactions on Electron Devices*, vol. 65, no. 1, pp. 115-121, Jan. 2018.

[22] T. Lee and J. H. Nickel, "Memristor Resistance Modulation for Analog Applications," in *IEEE Electron Device Letters*, vol. 33, no. 10, pp. 1456-1458, Oct. 2012.

[23] G. González-Cordero, M.B. González, H. García, F. Campabadal, S. Dueñas, H. Castán, F. Jiménez-Molinos, J.B. Roldán, “A physically based model for resistive memories including a detailed temperature and variability description”, in *Microelectronic*

Engineering, vol. 178, 2017, pp.26-29